EUROPEAN UNION
Institute for Security Studies

GUARDIAN OF THE GALAXY

EU cyber sanctions and norms in cyberspace

Edited by
Patryk Pawlak and Thomas Biersteker

With contributions from
Karine Bannelier, Nikolay Bozhkov, François Delerue, Francesco Giumelli, Erica Moret, Maarten Van Horenbeeck

CHAILLOT PAPER / 155
October 2019

European Union Institute for Security Studies (EUISS)

100, avenue de Suffren
75015 Paris

http://www.iss.europa.eu
Director: Gustav Lindstrom

print

ISBN 978-92-9198-849-5
CATALOGUE NUMBER QN-AA-19-005-EN-C
ISSN 1017-7566
DOI 10.2815/04457

online

ISBN 978-92-9198-850-1
CATALOGUE NUMBER QN-AA-19-005-EN-N
ISSN 1683-4917
DOI 10.2815/672270

Published by the EU Institute for Security Studies and printed in Belgium by Bietlot.
Luxembourg: Publications Office of the European Union, 2019.
Cover image credit: NASA/JPL-Caltech

EUROPEAN UNION
Institute for Security Studies

GUARDIAN OF THE GALAXY

EU cyber sanctions and norms in cyberspace

Edited by
Patryk Pawlak and Thomas Biersteker

With contributions from
Karine Bannelier, Nikolay Bozhkov, François Delerue, Francesco Giumelli, Erica Moret, Maarten Van Horenbeeck

CHAILLOT PAPER / 155
October 2019

Acknowledgements

This *Chaillot Paper* is the outcome of several months of reflection and discussions conducted in the framework of the EUISS Task Force on Restrictive Measures Related to Malicious Activities in Cyberspace (hereafter 'EUISS Task Force on Cyber Sanctions'). The Task Force met on numerous occasions between October 2018 and July 2019 and organised several focus group meetings with representatives of the EU institutions and member states. The content of this volume reflects only some of the discussions that took place during those meetings.

The editors would like to thank the following members of the Task Force for their contribution to several sections of this publication: Karine Bannelier (chapter 6), Nikolay Bozhkov (chapters 1, 2, 3), François Delerue (chapters 4 and 5), Francesco Giumelli (chapters 1, 3 and 8), Erica Moret (chapters 1, 3 and 8), and Maarten Van Horenbeeck (chapters 1, 5 and 8).

In addition, we would like to express our gratitude to all EU and member state officials for their inputs and comments. Finally, this volume has benefited from the work and input of EUISS colleagues: Florence Gaub and Clara Portela provided insightful comments on the text, Gearóid Cronin took care of the language editing, and Christian Dietrich created the infographics. As always, any mistakes or omissions are those of the authors alone.

The editors

Patryk Pawlak heads the Brussels office of the EUISS, where he is responsible for inter-institutional relations and coordination of cyber-related projects.

Thomas Biersteker is Gasteyger Professor of International Security and Director of Policy Research at the Graduate Institute, Geneva.

The EUISS Chaillot Paper series

The *Chaillot Paper* series, launched in 1991, takes its name from the Chaillot hill in the Trocadéro area of Paris, where the Institute's first premises were located in the building occupied by the Western European Union (WEU). The hill is particularly famous for the Palais de Chaillot which was the site of the signing of the UN Universal Declaration of Human Rights in 1948, and housed NATO's provisional headquarters from 1952 until 1959.

CONTENTS

EXECUTIVE SUMMARY

Cyberspace is not an ungoverned space. Existing international law and accepted norms of responsible behaviour provide clear guidance on what is and what is not permissible in cyberspace. And yet, states increasingly rely on cyber operations to achieve their political objectives and strategic goals: whether through industrial cyber-espionage to give competitive advantage to domestic companies, sophisticated operations to steal military secrets, or blatant attacks targeting the critical infrastructure of other states.

This widespread sense of impunity has driven the European Union and its member states to support regional and global efforts to ensure that the perpetrators of the attacks face the consequences and that their victims are adequately protected and compensated. The so-called Cyber Diplomacy Toolbox adopted by the EU in 2017 provided a significant boost to the Union's goal of becoming a 'forward-looking cyber player'. In addition to a number of diplomatic and operational measures, the toolbox proposed the use of sanctions as one of the instruments at the Union's disposal.

This *Chaillot Paper* – which uses space exploration as a metaphor to demystify some of the concepts and challenges linked to cyber-related policymaking – focuses on the EU's cyber sanctions regime as established by Council Decision 2019/797 and Council Regulation 2019/796. The EU's autonomous cyber sanctions regime – encompassing measures such as travel bans and asset freezes – represents a significant achievement on the EU's path to promote a free, open and secure cyberspace and defend the rules-based international order. However, the growing complexity of cyber threats and the proliferation of malicious actors intent on undermining the EU's global standing, as well as its economic power and political foundations, suggest that it is not yet the time for self-congratulation.

Taking account of the lessons derived from other sanctions regimes adopted by the EU in the past, this *Chaillot Paper* addresses a number of key issues relevant for ensuring the maximum effectiveness of the EU's cyber sanctions regime:

1. Clarity about the logic behind the use of cyber sanctions;
2. Potential impact of the sanctions on the EU's overall bilateral relations, and their interplay with other foreign and security policy instruments;
3. Objectives that specific listings aim to achieve;
4. Adequate timing and longevity of the listings;
5. Understanding of the target;
6. Sufficient capabilities and resources;
7. Mechanisms for coordination and information sharing;
8. Cooperation and coordination with international partners;
9. Engagement with the private sector;
10. Clear strategic communication.

In tackling these questions, the contributors to this publication provide insights into a number of complicated issues of a political and legal nature, including the challenges of attribution, state responsibility in cyberspace, the principle of due diligence or the potential impact of cyber sanctions on the physical world. The analysis concludes with a set of proposals aimed at stimulating the discussion about the implementation of the EU cyber sanctions regime – and which will hopefully lead to concrete actions.

INTRODUCTION

THE HEROINE AWAKENS

The EU as a sanctioning power

The Guardians of the Galaxy is an American movie production about the adventures of intergalactic superheroes who together fight to protect the galaxy from planetary threats. They succeed in vanquishing Ronan – a fanatical genocidal warlord seeking to undermine the peace treaty between the Kree Empire and the Nove Empire. They also slay the Abilisk – a multi-dimensional tentacled monster consuming the power resources of the Sovereign planet. Despite their different backgrounds, they form a unique alliance to save the galaxy.

So what is the link between a group of intergalactic heroes and the European Union? First, a strong desire to save their home. Like the fictional Guardians, the EU understands that ultimately there is no sanctuary from cyber threats. For this reason, strengthening your own capacities and those of your partners is often the best way forward. Like the Guardians, the EU's strength comes from the qualities and powers of its individual members – despite different personalities and distinctive individual character traits. Finally, the threats they face are constantly evolving – whether travelling through the galaxy or different jurisdictions of the sovereign states. In the absence of an effective protection mechanism, both the Guardians and the EU do their best to provide security and justice for all by bringing those accountable for misdemeanours to justice.

In this new era of interstate competition, the cyber domain is used by states as an equaliser for levelling the geopolitical playing field.

Monsters in cyberspace

Cyberspace is full of malicious computer worms and viruses whose sophisticated names resemble those of the villains in sci-fi movies. Stuxnet, a multidimensional giant worm first uncovered in 2010, was responsible for causing substantial damage to Iran's nuclear programme. In May 2017, a shape-shifting villain, WannaCry, affected more than 200,000 computers in over 150 countries causing extensive damage estimated at hundreds of millions of euro.[1] Several months later, the Danish shipping company A.P. Moller-Maersk, among others, suffered from an attack by NotPetya – a mutant version of WannaCry – that cost their business an estimated €200-300 million.

Beyond monsters and villains, there are often powerful puppet masters who are not averse to resorting to cyber tactics to pursue their strategic objectives. The year 2019 has seen an unprecedented level of state-run operations

1 It is difficult to estimate the exact cost of that attack – or of any cyberattacks in general. However, the UK Department of Health has released data suggesting that that specific cyberattack cost the National Health Service almost £100 million and led to the cancellation of 19,000 appointments.

in cyberspace driven by broader geopolitical considerations. For instance, the withdrawal of the United States from the Iran nuclear deal and the growing tensions between the two countries has not ended with the usual war of words but led to an open confrontation both in the physical world and cyberspace. Since the beginning of the year, Iranian hackers have reportedly ramped up their cyber activities around the world, in particular in the US.[2] The US, on the other hand, has admitted to carrying out a cyberattack against Iran's rocket and missile launch control systems as well as to another that wiped out a critical database used by Iran's paramilitary arm to plan attacks against oil tankers.[3] Similarly, responses to Russian-orchestrated disinformation and electoral interference campaigns in both Europe and the US have increasingly relied on cyber operations.[4]

Giving sanctions a good name

Countering the notion that in cyberspace one can operate freely and without any consequences, it is important to stress that cyberspace is not a lawless territory. On the contrary, the web of institutional, legal and policy arrangements addressing various dimensions of internet governance is dense. Yet, the borderless and transnational nature of cyberspace, the questions about jurisdiction and sovereignty which it raises, and the fragmentation of cyber-related policymaking contribute to an ambiguity that is frequently exploited by malicious actors. Relative anonymity in cyberspace and the lack of absolute certainty when pointing a finger at a suspected perpetrator provide a camouflage for interstate competition. In this new era of interstate competition, the cyber domain is used by states as an equaliser for levelling the geopolitical playing field – not always in accordance with international law or acceptable norms of behaviour in cyberspace.[5]

Consequently, the prevailing sense of impunity for violations of norms and international law has frustrated many, including the EU and its member states, leading to a quest for new strategies. Countries have opted for different, but complementary, approaches aimed at strengthening the robustness of norms and signalling the potential consequences incurred by those who violate them. The United Kingdom, for instance, has focused on increasing cyber deterrence based on four main pillars: (i) identifying the perpetrators and responding accordingly, including through public naming and shaming; (ii) exposing the mechanisms behind the attacks (in as much detail as possible), so as to thwart the attacker's ability to use similar methods in future campaigns; (iii) prosecuting those who have conducted attacks in line with cybercrime laws; and (iv) any other steps consistent with international law.[6] Several European states – like Estonia, France, the Netherlands and the UK - have taken steps to increase transparency in cyberspace by clarifying their official views on norms of responsible behaviour and/or the application of existing international law.[7] States have also increasingly resorted to coordinated public attribution as a means of shaming their perpetrators. The coalitions of states who pointed fingers at Russia's foreign military-intelligence agency GRU

2 Andy Greenberg, "Iranian Hackers Launch a New US-Targeted Campaign as Tensions Mount", *Wired*, June 20, 2019, https://www.wired.com/story/iran-hackers-us-phishing-tensions/

3 Julian E. Barnes, "U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say", *New York Times*, August 28, 2019, https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html.

4 Gabrielle Tétrault-Farber and Andrey Kuzmin, "Russia Thwarts U.S. Cyber Attacks on its Infrastructure: News Agencies", *Reuters*, June 17, 2019, https://www.reuters.com/article/us-usa-russia-cyber-russia/russia-thwarts-u-s-cyber-attacks-on-its-infrastructure-news-agencies-idUSKCN1TI1U0.

5 David E. Sanger, *The Perfect Weapon* (New York: Crown Publishing Group, 2018).

6 Foreign Office of the United Kingdom, Speech by Foreign Secretary Jeremy Hunt at the University of Glasgow, March 7, 2019, https://www.gov.uk/government/speeches/deterrence-in-the-cyber-age-speech-by-the-foreign-secretary.

7 See for instance the speech by Advocate General Jeremy Wright of the United Kingdom or the Strategic Review of Cyber Defence. A more extensive discussion on the role of strategies as normative documents can be found in: Eneken Tikk and Mika Kerttunen, "Strategically Normative: Norms and Principles in National Cybersecurity Strategies", *Research in Focus,* EU Cyber Direct, April 2019.

following the operation against the Organisation for the Prohibition of Chemical Weapons (OPCW) or at North Korea for WannaCry are good examples. The US, on the other hand, adopted in 2018 the doctrine of 'persistent engagement' and 'defend forward' – referring to an imperative for the US military to carry out activities aimed at intelligence collection and disruption or halting of malicious cyber activity at its source, including in response to activities below the level of armed conflict.

The move towards sanctions – which are generally perceived as having 'more teeth' than diplomatic statements and declarations – and increasing focus on imposing consequences on norm-violators are also closely linked to the general disappointment with the limited effectiveness of the existing normative frameworks for responsible state behaviour in cyberspace. It is here that the application of sanctions could potentially play a constructive role. Sanctions can be used to highlight, target and deter inappropriate behaviour, and since all sanctions invariably send normative signals, sanctions can be applied to bolster emergent norms, and to reinforce existing ones. In the European context, sanctions could be applied to support European core values and overarching goals of a free, open, stable and secure cyber domain.

Understanding sanctions

Sanctions are a policy instrument available to decision-makers attempting to change, to limit, or to criticise in normative terms the behaviour of another actor. Sanctions entail the application of specific tools to achieve concrete political goals or objectives, and they range in scale or breadth from comprehensive trade and financial embargoes (i.e. a complete blockade of all trade and financial transactions with an entire country) to limited numbers of individual designations. While often associated with economic restrictions, sanctions can also entail restrictions on flows of arms, the activities of diplomatic personnel, or the freedom of movement of individuals (travel bans).

Sanctions are rarely, if ever, used in isolation, and they are typically employed in combination with other policy instruments – negotiations or mediation, the threat or use of force, and/or referrals to legal tribunals. Policymakers do not ordinarily choose between sanctions and negotiations, because the two instruments are commonly employed simultaneously and because sanctions can be used as leverage in bargaining situations. Sanctions typically follow strong diplomatic statements, however, and can be employed to indicate the strength of conviction of the sanctioning body. They have more force, because they entail costs for both the targets and senders of sanctions. For instance, while the target of an individual asset freeze bears disproportionate costs, the imposition of such a sanction also entails significant compliance costs for financial institutions in the sending countries. In the case of travel bans, the cost is pushed onto travel companies or border authorities who also need to reinforce their capabilities.

Since all sanctions invariably send normative signals, sanctions can be applied to bolster emergent norms, and to reinforce existing ones.

While most of the sanctions literature and popular commentary evaluates sanctions in terms of their ability to coerce a change in the behaviour of a target, recent research has emphasised their multi-purpose nature.[8] Most sanctions regimes are motivated by an effort to **coerce** a change in behaviour: however, there are instances in which the target of sanctions is so committed to a cause (such as al-Qaeda or Daesh) or in which behavioural change could mean an existential crisis for the target (e.g. in cases of

8 Thomas J. Biersteker, Sue E. Eckert, and Marcos Tourinho (eds.), *Targeted Sanctions. The Impacts and Effectiveness of United Nations Action* (Cambridge: Cambridge University Press, 2016).

Responding to malicious cyber operations

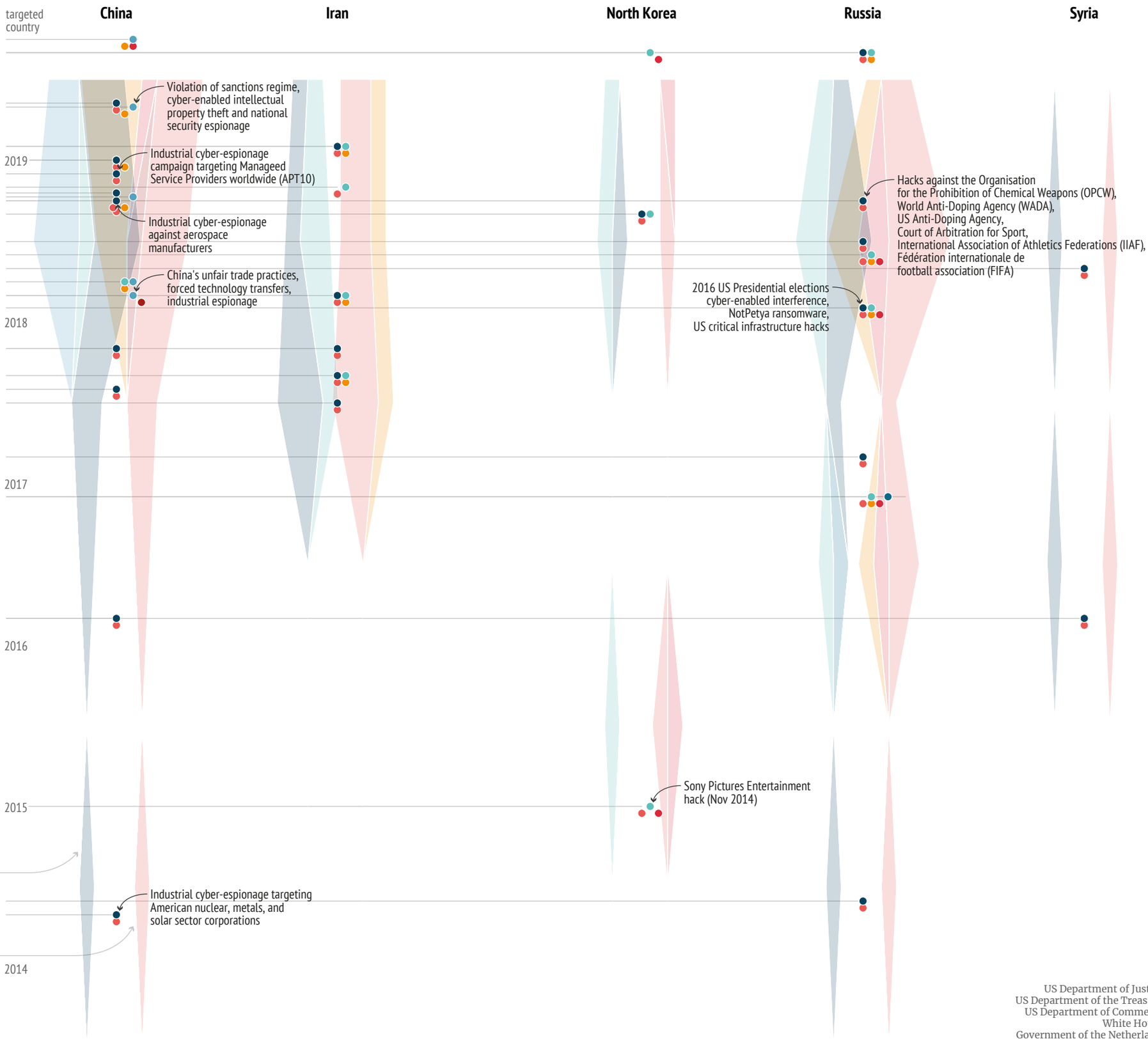
examples of measures adopted up to September 2019

This dataset tracks instances of targeted measures adopted primarily by the United States in response to cyberattacks, cyber-enabled incidents, and practices and acts with a cyber-domain component.

They are divided into categories depending on the target of sanctions: private/corporate entities, individuals or organs/organisations affiliated with, linked to, or acting at the behest of, third states. The four categories of measures illustrated here encompass: criminal indictments (law enforcement measures), financial sanctions (asset freezes and travel bans), trade sanctions (export and transaction control measures), and diplomatic responses (diplomatic expulsions and diplomatic visa restrictions). The number of entities, individuals or organs of the state subjected to those measures are tracked based on the supplementary documentation.

Linkages of targeted entities, individuals, organs or institutions to third states are based upon the open source information and reasoning provided by the sanctioning entities. Some instances of diplomatic measures respond to malicious cyber activities indirectly, only referencing them as substantiating criteria.

Grey lines connect to measures, cool colours describe the type of measure, warm colours describe a measure's target, dots break down any one measure, and polygons describe their cumulative amount per year.



Data:
US Department of Justice, 2019;
US Department of the Treasury, 2019;
US Department of Commerce, 2019;
White House, 2019;
Government of the Netherlands, 2018

'Sanctions' and 'restrictive measures'

In the European Union, these two terms – 'restrictive measures' or 'sanctions' – are used interchangeably. They constitute an essential tool of the EU's Common Foreign and Security Policy (CFSP). They are used by the EU as part of an integrated and comprehensive policy approach, involving political dialogue, complementary efforts and the use of other instruments at its disposal.

Sanctions are preventive measures which allow the EU to respond swiftly to political challenges and developments that go against its objectives and values. For instance, sanctions can target state actors that are guilty of: terrorism, nuclear proliferation activities, human rights violations, annexation of foreign territory, and the deliberate destabilisation of a sovereign country.

Sanctions seek to bring about a change in the policy or conduct of their addressees, with a view to promoting the objectives of the CFSP.

They can aim at:

> governments of non-EU countries that pursue policies that threaten or aim to destabilise the EU;

> entities (companies) providing the means to conduct the targeted policies;

> groups or organisations such as terrorist groups;

> individuals supporting the targeted policies, involved in terrorist activities etc.

Sanctions in a broad sense, or **diplomatic sanctions**, include actions such as the interruption of diplomatic relations with the targeted country, or the coordinated recall of diplomatic representatives of the EU and its member states.

Sanctions in a narrow sense require a specific legal base in the EU Treaties, and include:

> **arms embargoes**;

> **restrictions on admission** of listed persons (travel ban): targeted persons cannot enter the EU, or travel beyond their member state of nationality if they are an EU citizen;

> **freezing of assets** belonging to listed persons or entities: all their assets in the EU are frozen and EU persons and entities cannot make any funds available to those listed;

> **economic sanctions** or restrictions concerning specific sectors of economic activity, including import or export bans on certain goods, investment bans, prohibitions on supplying certain services etc.

Source: Council of the European Union, "Sanctions: how and when the EU adopts restrictive measures", https://www.consilium.europa.eu/en/policies/sanctions/

regime change) that the core purpose of sanctions is to **constrain** a target by raising the costs of its behaviour or forcing it to engage in costly changes of strategy. Sanctions also invariably send normative **signals** to targets. Every UN Security Council resolution, EU Council decision, or justification for unilateral sanctions measures contains a statement of the reasons for the application of the exceptional measures, with reference to the norms violated by the object or target of the sanctions. Each of these different facets is underpinned by a different operational logic: coercion attempts to change the cost/benefit analysis by increasing costs to the target; constraint aims to reduce the capabilities of the target by limiting its access to resources needed to continue its proscribed activity; and signalling articulates clearly what constitutes a norm violation and stigmatises those who violate such norms in particular social contexts.

Most sanctions are targeted in some form (i.e. unlike comprehensive trade and financial embargoes). All UN, EU, and most US sanctions

belong to the category of targeted sanctions. Targeted sanctions vary from being selectively targeted at only a small number of individuals, to including arms embargoes, diplomatic restrictions, and sectoral commodity bans, often on the sources of finance for arms purchases by combatants in armed conflicts. In some instances, the scope of application is widened to the entire economy, such as when sanctions are imposed on a country's financial sector or oil embargoes are introduced. Because they are more discriminating, targeted sanctions have the normative virtue of not punishing an entire population for the actions of a small governing minority. They also are more amenable to incremental manipulation than comprehensive sanctions, since they can be more readily ratcheted upwards or downwards in response to target behaviour in a bargaining situation.

In light of the limited effectiveness of the normative and legal frameworks in place, on one hand, and the growing reliance on cyber activities by both state and non-state actors – each with their own motivations – on the other, it is not surprising that sanctions have emerged as part of the toolbox that can be applied to change behaviour, constrain malicious activity, and signal norm preferences in the cyber domain.

Targeted sanctions have the normative virtue of not punishing an entire population for the actions of a small governing minority.

Cyber sanctions in the EU

Cyber sanctions – as addressed in this *Chaillot Paper* – refer to traditional measures (e.g. travel bans, asset freezes) used in response to malicious activities occurring in cyberspace. The EU's engagement in global cyber debates, its prominent role in shaping the digital environment worldwide, and strong normative stance have built up the expectation that the EU will assume a more active role as a guardian of a free, open, safe and secure cyberspace based on the respect for internationally agreed norms and rules of behaviour. The cyber sanctions regime established by the EU in May 2019 has further reinforced this sentiment among its international partners and audiences. Council Decision 2019/797 and Council Regulation 2019/796 put in place a framework for targeted sanctions 'to deter and respond to cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States'.[9] Other than the United States, the EU is now the only major international player to have proposed a set of concrete policy options to deal with irresponsible behaviour in cyberspace. Its regime of autonomous sanctions is one of the tools designed to strengthen the rule-based international order and ensure broader global adherence to the internationally agreed norms of responsible behaviour in cyberspace.

However, there is a considerable gap between the adoption of the regime and its full operationalisation. The discussion about concrete listings, the scope of the measures (e.g. whether they target individuals or corporate entities) and specific elements of this process – such as criteria and justification for listing – will be where theory meets practice. Consequently, many questions surrounding the new regime are still open: what are the norms that the EU's cyber sanctions regime will strengthen? Is there a hierarchy of norms that the EU is ready to defend as a matter of priority? What are the main challenges ahead linked to the listing process? And finally, are there any useful lessons that we can draw from other sanctions regimes in order to strengthen the effectiveness of the EU's newly-established regime?

9 Council of the European Union, "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States", *Official Journal of the European Union*, L 129I, May 17, 2019, p. 13-19; Council of the European Union, "Council Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States", *Official Journal of the European Union*, L 129I, May 17, 2019 pp. 1–12.

This *Chaillot Paper* addresses these and many other relevant questions. It builds on the deliberations of the EUISS Task Force on Cyber Sanctions that met between June 2018 and July 2019. Through interviews and focus group meetings with officials from the EU and member states as well as representatives of the technical community and private sector, we were able to dive deep into policy, legal and political questions linked to the EU's cyber sanctions regime. Ultimately, the body of work presented in this *Chaillot Paper* advances two main arguments.

> **The value of the EU's cyber sanctions regime depends, *inter alia*, on the Union's capacity to manage expectations and perceptions of this regime among its domestic audiences and international partners in order to achieve broader commitment to the existing norms of responsible behaviour in cyberspace.** As we demonstrate, there are still many political and legal challenges linked to the implementation of the new regime that need to be resolved, not least linked to the scope and nature of the listings and to evidentiary standards. These challenges need to be explained and addressed in order to ensure the buy-in by member states to implement the cyber sanctions regime through concrete listings. At the same time, both the partner countries and addressees of the sanctions regime need to have a minimum understanding of how the EU sanctions system works and what it can and cannot achieve.

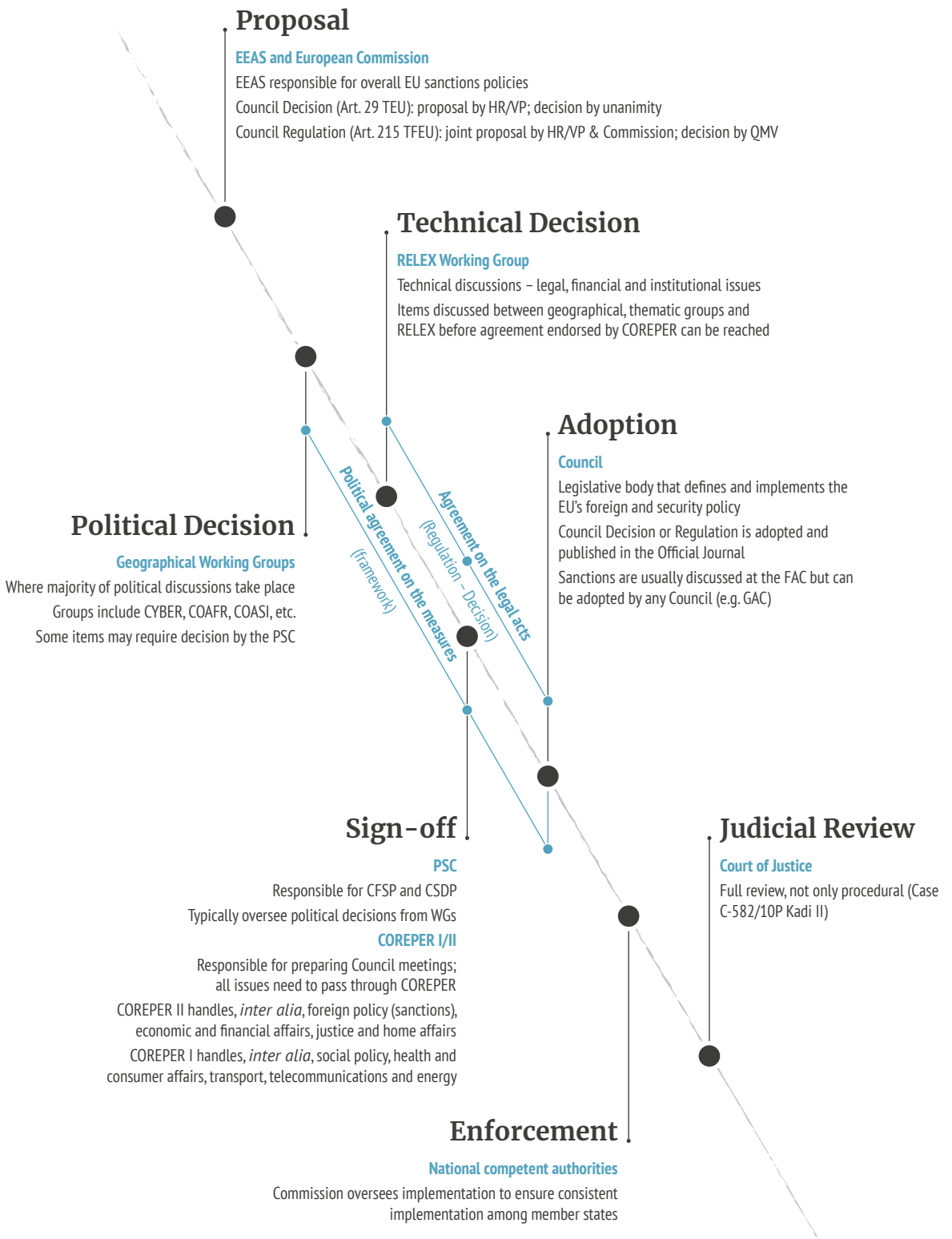
> **The EU's autonomous cyber sanctions regime constitutes a unique solution to the challenge of compliance with international law and norms of responsible state behaviour.** This is an important observation that needs to be taken into account when assessing the EU's cyber sanctions regime, in particular when it comes to the listing procedures, judicial review and evidentiary standards. As a political instrument governed by the rules of international law, sanctions, in general, are not subjected to the same level of judicial scrutiny regarding the evidentiary standards. However, the autonomous sanctions imposed by the EU are subject to judicial review by the Court of Justice of the European Union. This commitment to the due process, on one hand, and the political nature of the process whereby all member states need to agree unanimously to placing an individual or an entity on the sanctions list, on the other hand, is something that differentiates the EU from other actors but is not always clearly understood.

Different sections of this *Chaillot Paper* address precisely those issues and point to potential future dilemmas associated with the implementation of the EU's cyber sanctions regime. Ultimately, the key question that this collective volume addresses is: how do we make the EU's cyber sanctions regime effective?

To answer this question, the following chapters of this publication deal with its different dimensions. Taking into account the extensive scholarship on sanctions, chapter one looks at other sanctions regimes in order to identify lessons and past practices that influence the effectiveness of sanctions. The chapter establishes the list of ten questions that are addressed in the succeeding pages of this volume. As mentioned earlier, sanctions can play an important signalling role by providing an additional mechanism to make norms more robust. They are a means to end impunity in cyberspace, and promote accountability, transparency and a rules-based international order. But what exactly constitutes a violation of a norm and irresponsible behaviour in cyberspace that cyber sanctions aim to stigmatise? The answer to this question is provided in chapter two which examines various existing normative processes. Chapter three is the most relevant chapter for those interested specifically in the EU's cyber sanctions regime. It discusses the scope of the regime and procedures through which the regime will be implemented. It also signals potential challenges to the implementation of the regime, linked *inter alia* to the attribution of cyberattacks and evidentiary standards – a topic discussed in chapter five. Given the EU's commitment to the rules-based international order and multilateralism, we also found it necessary to address the question of the lawfulness of cyber sanctions from the international law perspective. Therefore, chapter four addresses the question of state responsibility and possible

Towards an EU sanctions regime

main stages and actors



Data: European Union

remedies under international law. Since the EU cyber sanctions regime and numerous earlier statements issued by Brussels not only prohibit certain types of activities but also oblige states to take concrete measures to prevent such activities from taking place on their territory, we have also included a chapter on the principle of due diligence that tackles this question. Chapter six explains in detail what this principle is and how it plays out in cyberspace. Recognising the fact that governance of cyberspace requires cooperation with other stakeholders, this *Chaillot Paper* devotes an entire chapter – chapter seven – to the role of the private sector as a norm entrepreneur and the role of public-private partnerships in evidence gathering, among other activities. Finally, chapter eight looks at the interplay of cyber sanctions with the physical world and potential consequences that they might have on the effectiveness of the law enforcement agencies in the fight against cybercriminals or cooperation between computer emergency response teams. This chapter also looks at the novel methods using cyber tools for sanctions evasion. We conclude by looking again at the initial set of ten questions presented in chapter one and make concrete proposals to increase the chances of success for the EU's newly-established cyber sanctions regime. This chapter highlights potential challenges but also offers concrete proposals to ensure better effectiveness of the adopted measures in order to make sure that the EU's cyber sanctions regime is not drawn into a huge 'black hole' created by political rivalries in (and over) cyberspace.

CHAPTER 1

NAVIGATING THE STARS

Ten questions to make cyber sanctions more effective

INTRODUCTION

In times of political instability and faced with serious security or foreign policy challenges, governments are under pressure to act. Sometimes, the decisions they take prove to be the right ones and politicians save their face in the court of public opinion. Sometimes, however, despite their good intentions, in the heat of the moment or under political pressure policymakers make mistakes or suboptimal decisions. Uncertainty about the policy outcome is an inherent part of policymaking. There are simply too many factors that determine the success of any given policy measures. The dilemma, however, is always the same: does it make more sense to do nothing and wait or is it better to take risks and take a concrete stand? Consequently, success and failure are inherent elements of foreign and security policymaking. One way to minimise the risk of failure is to learn from past experiences. This chapter looks at the existing scholarship on sanctions with a view to answering one simple question: which lessons might be useful to make the cyber sanctions regime more effective? These 'lessons learned' and the issues they identify will guide the analysis of the different aspects and dimensions of the cyber sanctions regime adopted by the EU.

DO SANCTIONS WORK?

Whether sanctions 'work' or not is the classic question raised about this commonly used tool of foreign and security policy. Although the question has been addressed in several studies over the past couple of decades, assessing the effectiveness of any given sanctions regime remains a challenge, given the difficulties in conclusively ascertaining a causal link between the imposition of sanctions and compliance or constraint. One thing is certain, however: sanctions are not a silver bullet solution for violations of international law or the enforcement of norms in cyberspace. Sanctions do not operate in a vacuum and the way in which they are combined with other tools of foreign, security and trade policy has a considerable impact on their ultimate effectiveness.[1] Identifying the effects of sanctions in isolation from other factors is a complicated, and sometimes impossible, task.[2] Many of those who maintain that

1 Margaret P. Doxey, *Economic Sanctions and International Enforcement* (Oxford: Oxford University Press, 1971); Robert A. Pape, "Why Economic Sanctions Do Not Work", *International Security*, vol. 22, no. 2 (1997): pp. 90–136; David A. Baldwin, "The Sanctions Debate and the Logic of Choice", *International Security*, vol. 24, no. 3 (1999/2000): pp. 80–107; Gary C. Hufbauer *et al.*, *Economic Sanctions Reconsidered* (Washington, DC: Peterson Institute for International Economics, 2007).

2 Erica Moret, "Humanitarian Impacts of Economic Sanctions on Iran and Syria", *European Security*, vol. 24, no. 1 (2015).

sanctions are not effective instruments are relying on a behavioural change approach, assuming that the target will adjust its policy or activities after the imposition of sanctions. However, this approach is now considered inadequate to account for the complexity of sanctions. A more nuanced analytical framework is therefore necessary in order to go beyond the limitations of the behavioural change paradigm.

Changing the behaviour of targets (*coercion*) certainly remains one of the principal objectives that sanctions are designed to achieve; however, this remains conditional on the political objectives of both the senders and targets being compatible. If senders and targets share economic or political interests and their mindsets align, then sanctions can be imposed to induce a change in behaviour. Otherwise, behavioural change becomes less likely. Sanctions can, nonetheless, fulfil other functions. When there is a lower likelihood of cooperation between targeted and sanctioning entities, then sanctions can be imposed to limit the possibility of the target embarking on an undesired course of action (*constraint*). This, for example, justifies the utilisation of sanctions against terrorist organisations/individuals, conflict spoilers and warlords. In such scenarios, sanctions are imposed as preventive mechanisms to make sure that certain events do not occur. Beyond coercing and constraining, sanctions also send strong messages of disapproval to different audiences (*signalling*) in order to shape their expectations about future events. Sanctions can warn targets about possible escalation, but they can also stigmatise certain types of behaviour as unacceptable in the eyes of an international audience. This means that sanctions play a powerful role in determining what norms and interests actors will have to take into account when making foreign policy decisions.

Sanctions are not a silver bullet solution for violations of international law or the enforcement of norms in cyberspace.

Studies evaluating the efficacy and impact of targeted sanctions imposed over the past 30 years conclude that sanctions are largely ineffective in achieving their stated aims, but have beneficial consequences in some circumstances.[3] The Targeted Sanctions Consortium (TSC) found that UN sanctions were effective in reaching their stated aims on average only 22% of the time, with a 28% success rate in constraining, a 27% success rate at sending effective signals, and a 10% success rate in coercing change in the target.[4] The emergence of targeted sanctions has contributed to altering the understanding of how sanctions function in at least three fundamental ways. First, the multitude of targets that can be listed at any given time creates the opportunity to pursue different objectives with a variety of people/entities at the same time. Second, a targeted sanctions regime is more easily malleable than a comprehensive sanctions regime. The mere adding or removal of several individuals can provide valuable leverage in a negotiation and alter the scope of the sanctions altogether. Finally, sanctioning powers can narrowly tailor the desired impact of targeted regimes to the salience of the problem at hand. This factor has contributed to making targeted sanctions a 'cheaper' option compared to other foreign policy alternatives. However, targeted sanctions have also been criticised for their lack of 'teeth', the evasion opportunities that they inherently offer, and, in the EU context, the rather complex decision-making process that precedes their introduction. This has been an especially strong criticism in comparison with sanctions regimes imposed by different actors (e.g. the US and UN). Ultimately, however, this has neither

3 Thomas Biersteker, Sue E. Eckert, Marcos Tourinho and Zuzana Hudáková, *The Effectiveness of United Nations Targeted Sanctions: Findings from the Targeted Sanctions Consortium (TSC)* (Geneva: Graduate Institute of International and Development Studies, 2013).

4 Targeted Sanctions Consortium (TSC), 2018, https://graduateinstitute.ch/research-centres/global-governance-centre/targeted-sanctions-initiative.

affected the expansion of sanctions nor the frequency with which they are utilised.

WHEN DO SANCTIONS WORK?

The absence of a sufficiently broad sample of previous examples of cyber sanctions makes it difficult to predict their future effectiveness. This does not mean however that we are navigating in uncharted waters without any guidance. Quite the opposite. Similar measures employed to tackle drug traffickers, criminal networks and terrorist cells can provide many useful lessons for heightening the efficiency of sanctions.[5] This section provides a 'checklist' with a constellation of questions that guide the analysis in the subsequent chapters of this *Chaillot Paper.*

Is the logic of the sanctions regime clearly defined?

The underlying rationale of the cyber sanctions regime should be clearly outlined.[6] This should include a determination of whether the sanctions are intended to *coerce* targets to change their behaviour, *constrain* their activities or access to resources, and/or *signal* to the target and other would-be cyber criminals activities in cyberspace that the sanctioning power will not tolerate.[7] Such a logic should be inherent in the sanctions planning process as well as in the communications surrounding their use. Research by the TSC suggests that sanctions, at least in the UN context, are most likely to be effective in the sphere of signalling, with constraining and coercing achieving lower success rates.[8] In the case of cyber sanctions, the perpetrators of attacks may be less concerned about being 'named and shamed' as part of a retaliatory response. Furthermore, as cyber criminals are unlikely to subscribe to the same types of norms as the senders of the sanctions, the stigmatising or isolating impact of the cyber sanctions regime may be more limited as compared to other regimes: indeed, becoming the target of such measures could be conceived by such malicious actors as 'a badge of honour.' Nevertheless, while the targets of sanctions in the cyber domain might not be dissuaded, other actors might well be. This occurs in a context where potential criminals may be deterred if consequences are to be expected as a result of certain actions. In light of the above, constraining malicious actors' access to required resources or seeking to coerce their behaviour may be more productive strategies given the uniqueness of the cyber ecosystem.

Is the coordination with other foreign policy instruments ensured?

EU sanctions should always be contextualised in terms of the bloc's wider foreign and security policy strategies and activities. Sanctions must always be combined with other policy tools if they are to succeed in some way. In the case of cyber sanctions, and as already foreseen by the Cyber Diplomacy Toolbox (CDT), this could include dialogue, trade talks, diplomacy, law enforcement, collaboration with other countries and multilateral institutions, cooperation with the private sector and, in some instances, covert counterattacks and military deterrence. A better understanding of how these various instruments interact is needed in order to improve our insights into how sanctions work in

5 Erica Moret and Patryk Pawlak, "The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime?", *EUISS Brief* no. 24, July 12, 2018.

6 Francesco Giumelli, "How EU Sanctions Work: A New Narrative," *EUISS Chaillot Paper* no. 129, May 2013,

7 Francesco Giumelli, "New Analytical Categories for Assessing EU Sanctions". *The international Spectator: Italian journal of international affairs*, vol. 45, no. 3 (2010): pp. 131–144.

8 TSC, 2018, *op. cit.*

practice. At the same time, creating links between different policy instruments and considering their interactive effects is key in order to avoid potential unintended consequences of sanctions.

Does the choice of specific sanctions support the stated objectives?

When the EU employs cyber sanctions, it is worth keeping in mind that certain types of sanctions can be more effective than others, and the way in which different foreign and security policy tools are combined also plays a crucial role in their success. Diplomatic sanctions, for example, tend to be less effective due to the fact that they do not generate immediate economic consequences.[9] Similarly, travel bans and asset freezes – two of the most common forms of EU targeted restrictive measures – can be easily circumvented, especially in the absence of other foreign policy and security measures.[10] The UN experience has also demonstrated that there is a certain threshold of measures beyond which the effectiveness of sanctions diminishes.[11] For instance, an optimal level appears to be that which targets key export commodities (apart from oil), or sizeable companies that affect entire sectors of a targeted economy. On the other hand, sanctions consisting of only one measure (such as flight restrictions, or individual sanctions measures, taken alone) are never effective.[12]

Is the timing and longevity of the sanctions adequate?

In general terms, sanctions applied over a shorter timespan have been shown to be more effective than long-term measures that allow the target to develop alternative commercial relationships, generate domestic substitutes for sanctioned goods or engage in sanctions-busting activities through the use of middlemen and front companies. In the case of UN sanctions, some 40% of assessed 'successes' in altering the behaviour of a target have tended to occur in the first 12 months of a sanctions regime. In around 60% of cases that are deemed 'failures', the sanctions regimes exceeded three years. As such, sanctions regimes should be designed to be flexible and should be regularly reviewed and adapted to changing conditions. This is particularly relevant for the cyber domain, where quicker adaptation of sanctions will certainly be required. Furthermore, particularly in cyberspace, sanctions that can be enacted quickly and without warning would have higher chances of success, as they would not allow the target to prepare alternative courses of action. As pointed out in a previous EUISS publication on this topic, '[u]nexpectedness can be achieved by contingency planning, short deliberations, quick implementation, the engagement of unexpected (non-traditional) sanction imposers, and the use of instruments (new types of sanctions or restrictive measures) that have not been used before'.[13]

9 Clara Portela, "The EU's 'Sanctions Paradox'," in *Stiftung Wissenschaft und Politik (SWP Comments)*, 18, 2007, pp. 1-8.

10 Ibid.

11 Thomas Biersteker and Marcos Tourinho, "Have UN Targeted Sanctions Worked?" in Sebastian von Einsiedel and George Lopez (eds.), *The Sanctions Enterprise: Assessing a Quarter-Century of UN Action for Peace, Security and Human Rights* (Cambridge: Cambridge University Press, forthcoming).

12 Ibid.

13 Iana Dreyer and José Luengo-Cabrera (eds.), "On Target? EU Sanctions as Security Policy Tools", *EUISS Report* no. 25, September 2015.

Do the sanctions demonstrate a detailed understanding of the target?

Obtaining a detailed understanding of targets is a particular challenge given the anonymity that characterises the cyber domain. In the case of sanctions imposed against state actors, factors such as their political and economic stability, level of democratic freedoms, membership in international organisations, global economic and commercial interconnectivity, and degree of resilience to vulnerabilities are all vital considerations in crafting sanctions with an increased chance of meeting their stated aims.[14] If the targeted entity is an individual, company or a website, then a detailed understanding of its financing and resourcing, as well as connections to wider networks and motivations, is essential prior to sanctions imposition. Depriving a targeted entity of its main sources of revenue can be a highly effective way of constraining activities in which it is engaged and which are deemed unacceptable to sanctioning powers.[15]

Are the foreseen capabilities and resources sufficient?

Considerable levels of expertise, sufficient investment and advanced capabilities are necessary in the efficient imposition, enforcement and monitoring of sanctions. This is likely to be particularly valid in the technically sophisticated and fast-changing cyber domain. Nevertheless, cyber expertise within member states varies broadly at present. Furthermore, sanctions practice in the EU, as well as in the UN, has historically been marred by under-resourcing, under-staffing and sub-optimal transfer of institutional knowledge.[16] This has improved somewhat in recent years with investments in sanctions capabilities in the European External Action Service (EEAS) and the European Commission as well as in the competent authorities of various member states. The recent involvement of the member states and the Commission in the working group on cyber issues is an example of how awareness and the culture of cybersecurity can be improved. Nevertheless, staff turnover means that EU officials and seconded national experts from EU member states may only work on sanctions or cyber policies for a limited period of time, then move on to different jobs. This inevitably has an impact on institutional memory and hence the effectiveness of the entire sanctions regime.

Do the existing mechanisms for coordination and information-sharing work?

The effectiveness of sanctions in the EU can be affected by the degree of political support from individual member states and different departments within sanctioning authorities. The EU's requirement for consensus among all member states has, on occasion, led to sanctions being diluted.[17] The pace of reaching agreements on sanctions can also vary depending on the preferences and interests of individual member states. Moreover, there may also exist barriers and silos between relevant teams working on sanctions in EU institutions,[18] which presents difficulties for coordination with other sanctioning powers (such as the US). These drawbacks could be mitigated by mechanisms or groupings to coordinate and monitor joint

14 Thomas Biersteker and Peter A. G. van Bergeijk, "How and When do Sanctions Work? The Evidence", in Iana Dreyer and José Luengo-Cabrera (eds.), "On Target? EU Sanctions as Security Policy Tools," *EUISS Report* no. 25, September 2015.

15 Ibid.

16 Mikael Eriksson, *Targeting Peace: Understanding UN and EU Targeted Sanctions* (Farnham: Ashgate, 2010)

17 Erica Moret, Evidence provided to the UK House of Lords EU External Affairs Sub-Committee on post-Brexit sanctions policy and defence/security cooperation with the EU, July 2017, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-external-affairs-subcommittee/brexit-sanctions-policy/written/70456.pdf.

18 Ibid.

working in this field, something which is not currently well-developed at the global level.[19]

Sanctions also often depend on the sharing of intelligence and other sensitive forms of information between state actors. This is of particular relevance for cyber sanctions, where certainty about attribution, and adherence to the principles of necessity and proportionality are key conditions for the legality of countermeasures adopted under international law.[20] Despite this, global efforts to confront cyber threats are currently hampered by issues such as reluctance to share sensitive information linked to cyber capabilities or vulnerabilities. Efficient cooperation and information-sharing between EU organisations (including the Hybrid Fusion Cell, Europol's EC3, the EU CSIRT network and ENISA) will positively influence the EU's ability to identify targets and craft proportionate sanctions in response.

How is multilateral engagement and coordination with partners ensured?

Studies show that the effectiveness of sanctions can be augmented when various major economic and political powers work together to avoid creating economic gaps that can be exploited by third parties, for evasion or trade diversion. This is particularly the case regarding financial sanctions or embargoes on particular commodities.[21] In the context of cyber sanctions, the US is the only other sanctioning power that has so far imposed its own restrictions. Nevertheless, others are likely to follow suit, which could enhance the effectiveness of the EU's own measures, particularly if measures are coordinated strategically and judiciously. This might include traditional sanctioning partners, such as Canada, Japan and Australia, non-EU European neighbours which traditionally align with EU restrictive measures (such as Iceland, Norway, Switzerland and Ukraine) or collaboration through other regional and *ad-hoc* groupings, such as the G7.

Are the mechanisms for cooperation with industry in place?

Close collaboration exists between the EU and the banking sector in the realm of targeted financial sanctions and compliance of financial institutions. This type of cooperation between the EU and the private sector could serve as a basis for developing a similar network on cyber sanctions.

Close cooperation with the private sector and technical communities through exchanges of information and good practices is of pivotal importance to ensure that the EU's cyber sanctions are sufficiently targeted, up-to-date and in line with the latest technological developments. This is especially relevant with regard to compliance, where the private sector can help shed light on the activities of targeted actors.

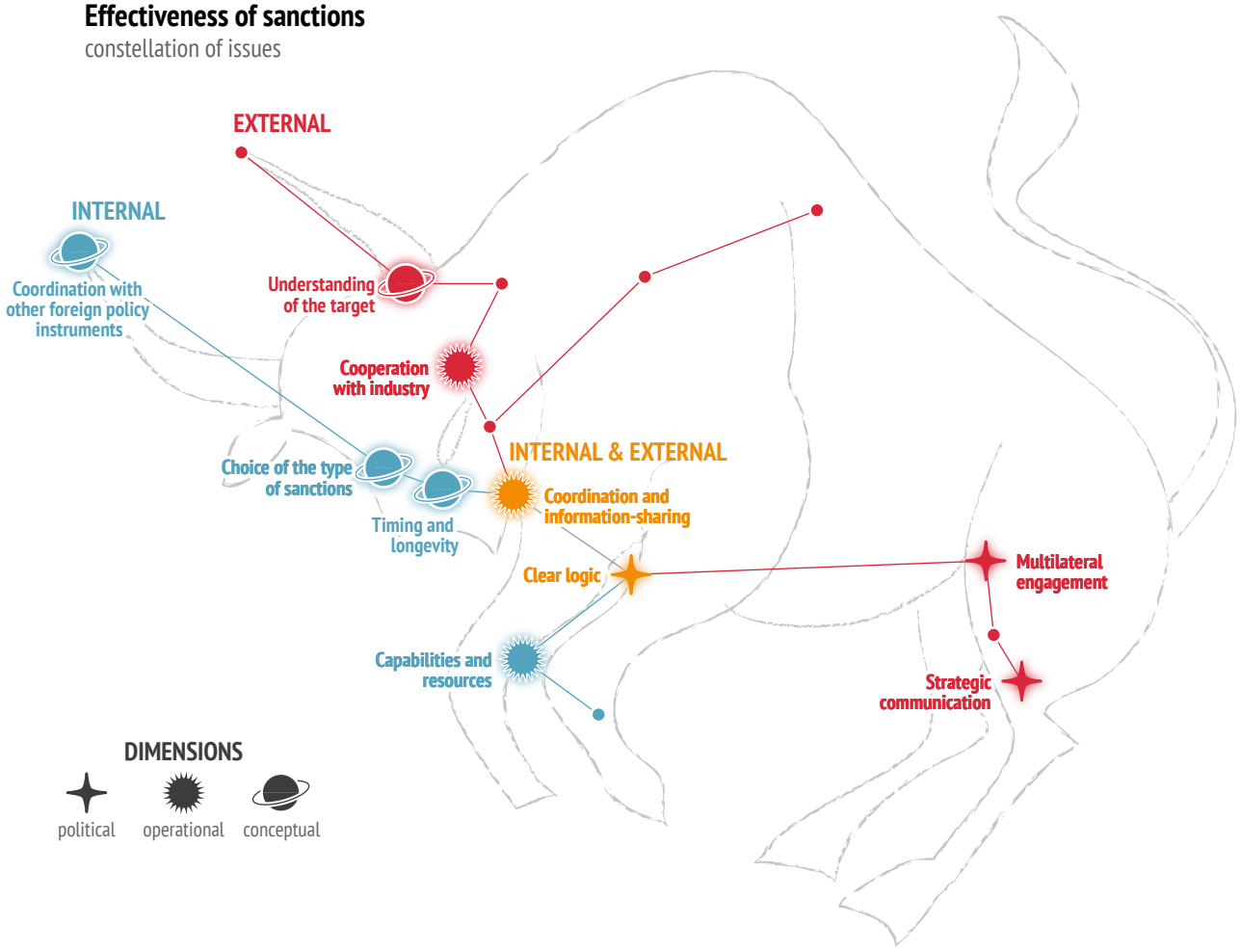
Is there a clear communication strategy?

Clear communication about the precise objectives of a given sanctions regime should be prioritised, especially given the potential reputational, economic and legal risks and costs that the imposition of a sanctions regime entails. In the cyber sanctions context, such costs may include a potential deleterious impact on domestic firms, a rise in corruption and criminality, in addition to a heightened probability of retaliation. Clear communication of purposes could also diminish 'rally-around-the-flag'

19 Erica Moret and Fabrice Pothier, "Sanctions After Brexit," *Survival: Global Politics and Strategy*, vol. 60, no. 2, (2018): pp. 179-200.

20 Erica Moret and Patryk Pawlak, *op. cit.*

21 Thomas Biersteker and Peter A. G. van Bergeijk, *op. cit.*



effects, where the government of the target of sanctions (i.e. an individual or corporate entity) garners popular support, or the strengthening of ties between the targeted entity and third countries or groups that may be deemed hostile to the senders of sanctions. The EU as a sanctioning power should also carefully consider the role played by the threat of adopting sanctions, given that a threat can sometimes have as, if not more, important an impact as the imposition of the sanctions themselves.[22] Companies and individuals also need to be properly and adequately informed on a continuous basis by those imposing sanctions, otherwise they will tend to change their operations in order to de-risk, which might inadvertently affect the effectiveness of policies in place. In general, poor communication undermines the legitimacy of the sending power and the effectiveness of the sanctions regime as a whole by reducing the number of actors, be they other countries or entities, willing to implement remedial measures or revert to an acceptable course of action.

22 Ibid.

CONCLUSIONS

The issues raised in this chapter and the proposed questions suggest that valuable lessons can be drawn from the sanctions regimes established in other policy areas. However, they cannot be applied automatically and need to be adjusted for the cyber context. Imposing sanctions in the cyber world presents a few differences from the imposition of conventional sanctions that are worth highlighting. First, sanctions in the cyber domain are more likely to deter states, but they are less likely to deter individuals from acting in the name of states. Second, the implementation and enforcement of sanctions in cyberspace require more developed skills than 'conventional' sanctions. These should be either acquired by states and/or drawn from the private sector. Third, sanctions in the cyber world are likely to fall short of the initially stated objective (e.g. a change in behaviour), which can increase their unintended effects (e.g. the target of the sanctions adopts an even more aggressive posture). Consequently, sanctions need to be designed in a way that allows for timely adjustments and changes. Special provisions for a cyber sanctions regime might need to be considered in order to address this matter. Thus, in principle, the effectiveness of sanctions in the cyber world can be assessed with a similar logic to that applied to sanctions in the 'conventional' world. However, due to the rapidly changing nature of the problem/actors and the absence of borders in cyberspace, a sufficient level of effectiveness can be reached only if international cooperation is enhanced both in terms of depth and quality.

The checklist presented above points to a number of issues that can be organised according to their thematic focus (i.e. conceptual, operational and political) as well as the target audience (i.e. internal and external – see diagram on previous page). In order to better understand the drivers behind the success and failure of a specific sanctions regime and to ensure its effectiveness, it is important to properly identify and assess the assumptions and concepts underpinning the design of the regime (e.g. interaction with other foreign policy tools, type of sanctions used, or a deep understanding of the target), its operational aspects (e.g. coordination and information-sharing mechanisms, capabilities and resources), as well as the political choices involved (e.g. logic of intervention, strategic communication). At the same time, each of these aspects is addressed to internal or external audiences driven by different motivations: political buy-in, better understanding of potential consequences for the parties involved, and awareness of the required resources and capabilities, among others. The subsequent chapters of this *Chaillot Paper* seek to help the reader navigate these complex questions and issues.

CHAPTER 2

CYBERSPACE DEBRIS

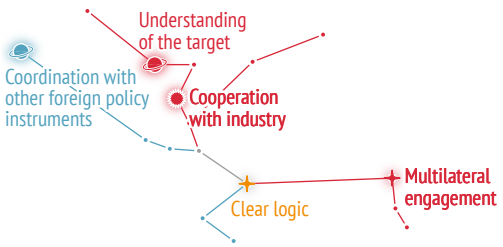
Sanctions and responsible state behaviour

INTRODUCTION

Cyberspace is littered with man-made debris: insecure products leaving assembly lines, the machines and data destroyed by cyberattacks, or armies of zombie computers (botnets) used to perform malicious attacks under remote direction. Most of it, if not all, is caused by irresponsible human activities: companies releasing machines and software with inadequate security protection, citizens not following the basic rules of cyber hygiene, or states pursuing their interests through malicious activities against other states.

The human origin of this problem suggests that the solution should also come from a change in human behaviour, including through defining clear norms of responsible state behaviour. Several such normative processes have been launched at global and regional levels – both by state and non-state actors – especially in the past five years. However, we have seen little improvement in the general situation. Quite the contrary, in fact: the use of internet infrastructure for offensive state operations has intensified, increasing the threat to international peace and security. Other forms of irresponsible behaviour include targeting of critical infrastructure and EU citizens, or undermining democracies and international institutions and organisations. It is not surprising therefore that the focus has increasingly shifted towards mechanisms for ensuring a broader compliance with the emerging or existing norms. In addition to the usual diplomatic tools – such as démarches or statements – cyber sanctions have emerged as an instrument with a real power to deliver the message, as opposed to just sending it.

Constellation of issues in this chapter



Consequently, the purpose of this chapter is to clarify the normative underpinnings of the discussion about cyber sanctions and to demonstrate their potential as a signalling tool. The chapter shows that despite the dynamic development of normative processes established by state and non-state actors regarding responsible behaviour in cyberspace, norm violations are still common. In such a context, sanctions – due to their impact through concrete restrictive measures (e.g. travel bans, asset freezes) – can play an important role as a compass, or at least as a signalling tool. The specific questions that this chapter aims to answer relate to the general debate about sanctions as a signalling mechanism: what drives the sanctions logic in cyberspace? How does the signalling

logic of sanctions fit within the broader discussion about responsible behaviour in cyberspace? How do sanctions fit within the broader set of foreign policy instruments? Who are the relevant stakeholders? What role does strategic communication play in this process?

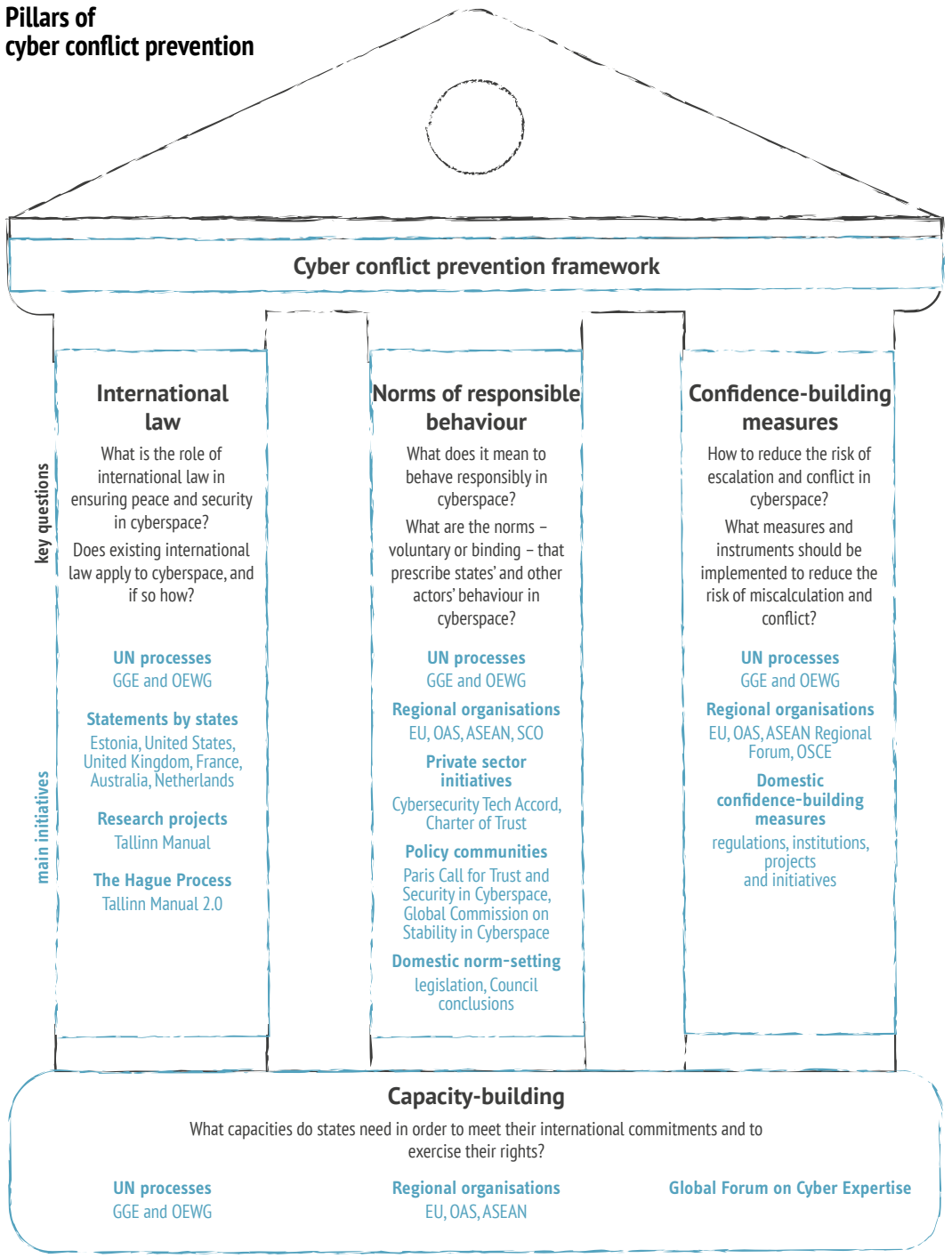
NORMATIVE SIGNALLING THROUGH SANCTIONS

The prevailing view regarding the usefulness of sanctions focuses on their contribution to bringing about a change in policy or activity by a targeted country, government, entity or an individual. One of the least explored aspects of sanctions is their role in sending normative signals – both to the target and to the larger international community. Not all sanctions are intended to coerce or constrain a target, but they are all intended to send normative signals.

Policy practitioners have indicated that sanctions are often applied to respond to political pressure 'to do something' about a dispute or an inappropriate act. Doing nothing would be tantamount to being complicit in the action and could inadvertently reinforce the behaviour judged to be aberrant. Practitioners want to do more than simply issue strong diplomatic objections or statements, but at the same time, they often consider the use of force as impractical, unwise, or both. In such instances, sanctions can be the most appropriate policy response. Sanctions can therefore play an important role as a powerful communication mechanism. Besides signalling general criticism of the violation of particular norms, they also reinforce the discursive condemnation with sanctions that can be costly for both the target and the sender. For instance, trade restrictions between two states, even if sector-specific, still have consequences for both parties. Thus, the application of an economic sanction signals strength of resolve. A sending party feels so strongly about the violation of a norm that it is willing to bear the economic costs of its sanctions on its own, and even face retaliation by the target. Ultimately, sanctions are not mere token gestures or 'cheap talk', but measures backed by a readiness to bear material and political consequences. The signalling dimension of sanctions has often been dismissed by scholars as merely 'symbolic', and it is indeed enormously difficult to measure the effectiveness of signalling.[1] That should not, however, prevent analysts from endeavouring to explore the clarity of the message being sent (which can be done from an analysis of the content of the texts of Council decisions authorising sanctions) or the degree to which targets are stigmatised in some settings or contexts (in effect, assessing the social impact of the signalling effort).

The potential use of sanctions in such contexts would be consistent with the EU's past practice of promoting human rights and supporting democratic processes and the rule of law, in contrast to the UN approach which is primarily focused on armed conflicts, terrorism, and proliferation, as well as support to transition processes. Nonetheless, the reinforcement of norms that are codified in national legislation and policies – albeit possible by means of law enforcement and prosecution methods – has also proven to be more of a paper tiger as none of the individuals indicted to date has been brought to justice (mainly due to the lack of cooperation from their home country). As such, the long arm of sanctions – as a coercive, constraining and/or signalling tool – remains a promising mechanism for response and deterrence, as well as creating, establishing, and strengthening norms.

1 Margaret Doxey, "International Sanctions: a Framework for Analysis with Special Reference to the UN and Southern Africa", *International Organization*, vol. 26, no. 3 (1972): p. 535; James Lindsay, "Trade Sanctions as Policy Instruments: A Re-Examination", *International Studies Quarterly*, vol. 30, no. 2 (1986): pp. 153-73; Thomas Biersteker, "UN Sanctions as Normative Signals", Paper presented at the 2016 meeting of the International Studies Association in Atlanta.


Pillars of
cyber conflict prevention
Cyber conflict prevention framework
key questions
main initiatives
International law
What is the role of international law in ensuring peace and security in cyberspace?
Does existing international law apply to cyberspace, and if so how?
UN processes
GGE and OEWG
Statements by states
Estonia, United States, United Kingdom, France, Australia, Netherlands
Research projects
Tallinn Manual
The Hague Process
Tallinn Manual 2.0
Norms of responsible behaviour
What does it mean to behave responsibly in cyberspace?
What are the norms – voluntary or binding – that prescribe states' and other actors' behaviour in cyberspace?
UN processes
GGE and OEWG
Regional organisations
EU, OAS, ASEAN, SCO
Private sector initiatives
Cybersecurity Tech Accord, Charter of Trust
Policy communities
Paris Call for Trust and Security in Cyberspace, Global Commission on Stability in Cyberspace
Domestic norm-setting
legislation, Council conclusions
Confidence-building measures
How to reduce the risk of escalation and conflict in cyberspace?
What measures and instruments should be implemented to reduce the risk of miscalculation and conflict?
UN processes
GGE and OEWG
Regional organisations
EU, OAS, ASEAN Regional Forum, OSCE
Domestic confidence-building measures
regulations, institutions, projects and initiatives
Capacity-building
What capacities do states need in order to meet their international commitments and to exercise their rights?
UN processes
GGE and OEWG
Regional organisations
EU, OAS, ASEAN
Global Forum on Cyber Expertise

Voluntary, non-binding norms, rules or principles of responsible behaviour of states

Norms reinforcing cooperation

- States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are harmful or may pose threats to international peace and security;
- States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats;
- States should respond to appropriate requests for assistance by another state whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity emanating from their territory.

Norms building trust

- In the event of ICT incidents, states should consider all relevant information, including the larger context of the event, the challenges of attribution and the nature and extent of the consequences;

Norms resulting from existing international law

- States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs (due diligence);
- States should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age (full respect of human rights).

Norms strengthening resilience and due diligence

- States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;
- States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities;
- States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.

Norms of restraint

- States should not conduct or knowingly support activity to harm the information systems of the authorised emergency response teams of another state. A state should not use authorised emergency response teams to engage in malicious international activity;
- A state should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.

Source: Based on Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015.

FINDING POLARIS: NORMS DEVELOPMENT AND PRINCIPLES OF CYBERSPACE NAVIGATION

The next obvious question is: do norms play a bigger role in cyberspace where laws are insufficient to constrain state behaviour, but which, if violated, necessitate a response?[2] Scholars have argued that some form of 'governance through norms' is needed where international law may apply in principle but is contested in practice. International norms are a useful device to interpret international law and regulate state behaviour when traditionally binding instruments are absent.[3] International norms are neither permanent nor fixed. Rather, they need to be constantly affirmed in order to remain viable as norms. They are re-articulated, re-performed, and re-stated through both discourse and action.[4] Existing international norms of non-intervention in the affairs of others (in support of sovereign non-intervention), or those prohibiting the use of force to resolve disputes, military aggression on the territory of neighbouring states, and the use of torture are codified in the Charter of the United Nations and in the Geneva Conventions.

States have developed multilateral arrangements – coalitions of the willing in cyberspace – that express their commitment to advancing responsible state behaviour.

These could be weakened as international norms in cases of non-adherence by states and failures to acknowledge violations by others. In this way, norms are statements of identity and core beliefs. That is manifested by the hortatory introductory paragraphs of UN Security Council resolutions, which contain and repeatedly underscore multiple signals, norm re-articulations, and strategic communications. Acknowledging norms of responsible state behaviour as powerful drivers for reducing risks to international peace and security, different global and regional organisations have taken steps to clarify the normative framework in cyberspace to reflect the expectations of the international community, shape the parameters of responsible state behaviour, and allow for assessments of activities and intentions of states.[5]

And yet, finding Polaris – that fixed point from which to draw measurements for cyberspace navigation – has proven difficult for many state and non-state actors alike. The following sections provide an overview of the ongoing initiatives focused on responsible behaviour in cyberspace and demonstrate how existing practice deviates from those normative commitments. Against this background, the chapter shows, sanctions have emerged as a meaningful tool for conducting foreign and security policy.

2 See: Xymena Kurowska, "The Politics of Cyber Norms: Beyond Norm Construction Towards Strategic Narrative Contestation", *Research in focus*, EU Cyber Direct, March 2019; Zine Homburger, "Conceptual Ambiguity of International Norms on State Behaviour in Cyberspace", *Research in focus*, EU Cyber Direct, March 2019.

3 Xymena Kurowska, *op. cit.*

4 Sarah Percy, "Mercenaries: Strong Norm, Weak Law", *International Organization*, vol. 61, no. 2 (2007): pp. 367-97.

5 In that sense, responsible behaviour is understood more broadly than the notion of state responsibility as a principle of international law.

UN-led processes

Over time, the discussions of the five reincarnations of the UN Group of Governmental Experts (UNGGE) on Developments in the Field of Information and Telecommunications in the Context of International Security have led to the adoption of eleven cyber norms embedded in the 2010, 2013 and 2015 consensus reports and endorsed by the UN General Assembly. The same UNGGE reports have concluded that existing international law, including the UN Charter in its entirety, applies to cyberspace. This conclusion reaffirms the rights and obligations of states under international law, including that of resorting to countermeasures and various methods of retorsion in the event of a cyber-attack. The UN-led process has been hijacked by big power politics – primarily the competition between the US and Russia – resulting in the adoption of two competing resolutions in December 2018 and the launch of two parallel processes: a new UN Group of Governmental Experts (due to conclude its work in 2021) and the Open-ended Working Group (expected to present its report in the summer of 2020).

Regional, multilateral and bilateral arrangements

Several UNGGE norms have been subsequently endorsed by other regional and thematic groupings. The third ASEAN Ministerial Conference on Cybersecurity in 2018 agreed to subscribe in principle to the 11 voluntary, non-binding norms recommended in the 2015 UNGGE Report, as well as to focus on regional capacity-building in implementing these norms. The G-7 Summit in Japan in 2016 adopted the Principles and Actions on Cyber followed by a Declaration on Responsible State Behaviour in Cyberspace in 2017, which not only reiterated the commitment to the norms package proposed by the UNGGE in 2015 but also proposed a new norm against industrial cyber-espionage.[6] Regional groupings such as the BRICS have also addressed the question of a normative framework for cyberspace. The 2017 BRICS Leaders Xiamen Declaration reiterated the central role for the UN in developing universally accepted norms of responsible state behaviour in the use of ICTs to ensure a 'peaceful, secure, open, cooperative, stable, orderly, accessible and equitable ICT environment.' The statement emphasised the paramount importance of the principles of international law enshrined in the Charter of the United Nations, particularly those of state sovereignty, the political independence, territorial integrity and sovereign equality of states, non-interference in the internal affairs of other states and respect for human rights and fundamental freedoms. In addition, several normative commitments – in particular one to abstain from attacks against each other's critical infrastructure – were incorporated in bilateral agreements between states such as the ones concluded by US-Russia (2013), China-Russia (2015), US-China (2015), and US-Japan (2019). Furthermore, states have developed multilateral arrangements – coalitions of the willing in cyberspace – that express their commitment to advancing responsible state behaviour. For instance, nearly 30 states signed the Joint Statement on Advancing Responsible State Behaviour in Cyberspace released ahead of the UN General Assembly debate in September 2019, committing themselves to working together on a voluntary basis to hold states accountable, including by taking measures that are transparent and consistent with international law.

Domestically-derived norms play an important signalling role with regard to states' expectations of what is acceptable or not in their relations.

6 The proposed norm states that "no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."

Cyber Diplomacy Toolbox

Clearly signalling the possible consequences of a cyberattack plays an important role in deterring or discouraging potential attackers. Based on this assumption, the Netherlands Presidency of the Council presented in 2016 a non-paper laying down a series of options for a diplomatic response to cyber operations. The non-paper received the endorsement of the Political and Security Committee (PSC) which requested the European External Action Service to elaborate on the matter further. In February 2017, the EEAS presented a Joint EEAS-Commission services issue paper on a joint EU diplomatic response to cyber operations, commonly referred to as the EU Cyber Diplomacy Toolbox.

A non-exhaustive list of the available instruments includes:

- Statements by the Council and High Representative condemning certain types of activities or expressing concerns about overall trends;
- Council Conclusions on developments in cyberspace that the member states consider important for peace and security or the protection of the EU's strategic interests;
- Joint requests for technical assistance through diplomatic channels in cases where several member states are affected by an incident;
- Diplomatic démarches by EU delegations and embassies of the EU member states aimed at obtaining support for a specific course of action taken by the European Union or requesting support in mitigating a particular risk;
- Bilateral and multilateral thematic and political dialogues with third countries and international/regional organisations, including cyber dialogues but also meetings between high-level home affairs or digital market officials, to discuss worrying trends and possible responses to malicious cyber activities;
- Restrictive measures (sanctions) against third countries or more targeted measures against individuals and entities adopted on the basis of the Council decision (Article 29 TEU) and Council regulation (Article 215 TFEU).

The approach received the full support of the member states with the adoption of the Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox') in June 2017.

Norms embedded in national laws and regulations

In addition to normative processes at the global and regional level, norms can be derived from national laws and regulations (primary autonomous norms), which reflect a given state's normative commitments and provide a concrete action plan through which a government intends to ensure compliance. Norm formation could be achieved, for instance, by imposing certain concrete legislative standards, or through the implementation of specific laws (e.g. laws that criminalise certain types of behaviour or actions with specific penalties attached). Primary autonomous norms can be traced throughout various policy domains, including data protection, human rights, trade, internal market, home affairs or foreign and security policy. For instance, the General Data Protection Regulation foresees financial fines for violations of the right of a person to privacy and data protection, and the EU Cybersecurity Act ensures the implementation of the 'security-by-design' principle for any equipment used in EU territory by use of a certification scheme with an added oversight.

In parallel, secondary autonomous norms emerge through the incorporation of norms elaborated at the global or regional level – such

as norms agreed at the UN level – in domestic legislation. As an example, the UNGGE norm requiring states to 'consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs', is 'implemented' in the EU through the criminalisation of illegal access to information systems, system and data interference, and interception;[7] the imposition of criminal punishment for basic offences (maximum of at least 2 years imprisonment), and in aggravating circumstances (organised crime, use of botnets, and when ID-theft is used);[8] and the establishment of competent authorities at the national and European level (e.g. the European Cybercrime Centre, ENISA) which can serve as information-sharing hubs, coordinators and providers of assistance.

The downside of a domestically driven approach is that it naturally reflects national interests and results in a *de facto* fragmentation of the international normative order, which in turn, results in further contestation. Nonetheless, domestically-derived norms play an important signalling role with regard to states' expectations of what is acceptable or not in their relations. China and Russia have both put in place strict laws that restrict free access to information by adhering to the norm of social stability and order over that of freedom of expression. The US has adopted sanctions and has issued criminal indictments against individuals, government and corporate entities to crystallise which actions it deems unacceptable, or at odds with global norms (as evidenced by the Mueller investigation into Russian interference in the 2016 US election and the criminal indictments issued).

EXPLORING THE EUROPEAN WAY

A target of malicious activities and a victim of cyberspace debris, the EU has invested in the development of its own framework for promoting responsible behaviour in cyberspace and specific measures to ensure compliance with this framework. Through its cyber *acquis*, carefully drafted over several years, the EU has sent a clear message about the normative framework in cyberspace that it wishes to support: a rules-based order based on the application of international law and adherence to voluntary norms of responsible state behaviour in peacetime.

In 2015, the Council concluded that to mitigate threats stemming from cyberspace and reduce the risk of conflict therein, the EU needed a comprehensive approach to cyber diplomacy using the full spectrum of diplomatic and legal instruments at its disposal.[9] Based on the assumption that signalling the likely consequence of a cyberattack would dissuade potential attackers, the Cyber Diplomacy Toolbox (CDT) includes instruments for cyber incidents response and specific actions to influence long-term behaviour and deter malicious cyber operations. Furthermore, the EU has agreed that the Cyber Diplomacy Toolbox could be used 'to prevent or respond to malicious cyber activities which may originate from a state or non-state actor or transit through a States' territory, if that State knowingly allows its territory to be used for such activity or knowingly supports it'.[10] The adoption of the Cyber Diplomacy Toolbox (CDT) was followed by the Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities presented in October 2017.

7 European Parliament and Council of the European Union, "Directive 2013/40/EU of the European Parliament and the Council on attacks against information systems", Brussels, August 12, 2013.

8 European Parliament and Council of the European Union, "Directive 2016/1148 of the European Parliament and the Council concerning measures for a high common level of security of network and information systems across the Union", Brussels, July 7, 2016.

9 Council of the European Union, *Draft Council conclusions on Cyber Diplomacy*, Brussels, February 11, 2015.

10 Council of the European Union, *Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities,* Brussels, October 9, 2017.

UN cyber norms

implementation in the EU (selected)

Norms of responsible state behaviour

Implementation in the EU

'Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security'

UNGGE 2015, 13a

EU Cybersecurity Strategy: 2013 and 2017

Actions countering malicious activities in cyberspace aimed at undermining the EU's interests and values, including sanctions (Cyber Diplomacy Toolbox)

Recalling principles of international law, including due diligence (Council conclusions on malicious activities in cyberspace, 2018)

'States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions'

UNGGE 2015, 13g

Establishment of the EU-wide certification framework

'Duty of care' principle to reduce product and software vulnerabilities and promotion of a 'Security by design' approach

Real-time requirements for protection of energy infrastructure components (2019)

Compendium on the cybersecurity of election technology (2018)

'States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect'

UNGGE, 13h

Criminalisation of illegal access to information systems, system and data interference, interception (Directive on attacks against information systems, 2013)

Establishing competent authorities at the national level (NIS Directive), European Cybercrime Centre, ENISA, etc.

Criminal sanctions for basic offences (max of at least 2 years), and in aggravating circumstances (organised crime, use of botnets, and when ID-theft is used) (NIS Directive)

'States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty'

UNGGE, 13h

Setting up Computer Emergency Response Teams (CERTs) (NIS Directive)

Blueprint for rapid emergency response (2018)

An obligation for 24/7 contact points to respond within 8 hours to urgent requests for help; and obligation to collect statistics on the offences (NIS Directive)

Data: European Union; United Nations

The document defines the respective roles of EU institutions and the Commission services, including mechanisms for adoption of the measures, preparatory processes and communication procedures.

Between 2017 when the CDT was adopted and November 2019, the tools listed in the document were used on three different occasions reinforcing the EU's commitment to certain norms:

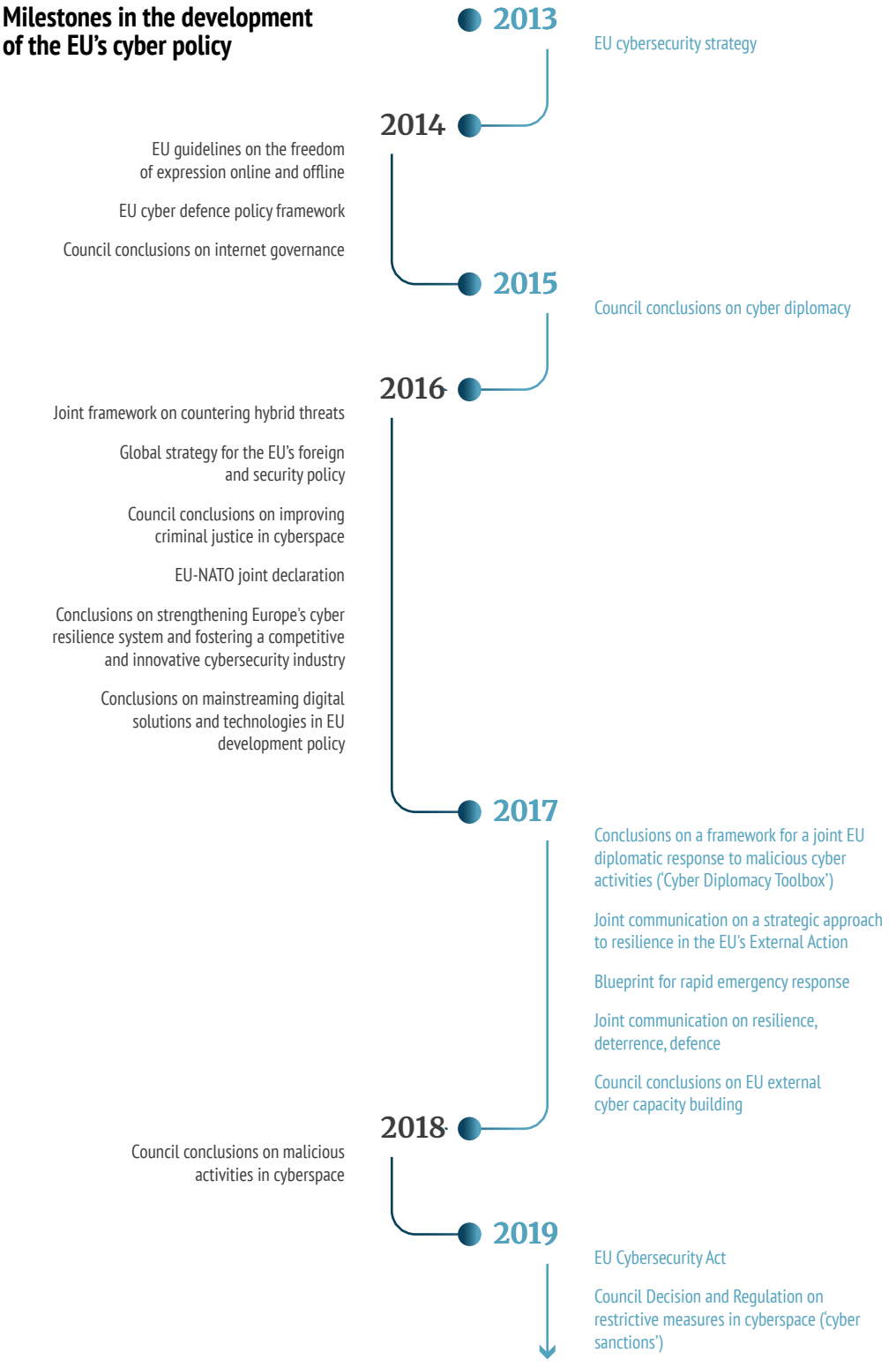
- Council conclusions on malicious cyber activities in which the Council stresses that the use of ICTs for malicious purposes is unacceptable and recalls the EU's commitment to further development and implementation of voluntary non-binding norms, rules and principles for responsible state behaviour in cyberspace as articulated in the 2010, 2013 and 2015 reports of the respective UNGGE, within the UN and other appropriate international fora. The document also states clearly that states should not conduct or knowingly support ICT activities contrary to their obligations under international law, must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-state actors to commit such acts.
- Joint statement by President of the European Council Donald Tusk, President of the European Commission Jean-Claude Juncker and High Representative Federica Mogherini concerning cyber-attacks against the Organisation for the Prohibition of Chemical Weapons (OPCW) in The Hague in a hostile cyber operation carried out by the Russian military intelligence service (GRU). The EU recalled that such activities undermine international law and international institutions and that it will continue to strengthen the resilience of its institutions and those of its member states.
- Declaration by the High Representative on behalf of the EU on respect for the rules-based order in cyberspace in which she expresses concern about 'the rise in malicious behaviour in cyberspace that aims at undermining the EU's integrity, security and economic competitiveness, including increasing acts of cyber-enabled theft of intellectual property'. The declaration also notes the EU's resolve to neutralise such malicious activities, including through co-operation with international partners.

SANCTIONS AND NORMS ENFORCEMENT

The EU's cyber sanctions regime was put in place only in 2019, which makes the use of cyber sanctions a relatively recent phenomenon. The US government began using sanctions to systematically respond to cyberattacks as of 2014. Beginning with its sanctions on North Korea for the SONY hack in 2014, it has employed targeted measures, including sanctions on individuals, private or government-affiliated corporations, and government agencies, and has reinforced those with the imposition of criminal indictments and diplomatic expulsions. To date, the EU member states have only utilised diplomatic expulsions, particularly in the context of the cyber-enabled attack against the OPCW. In comparison with sanctions in other policy areas, the US has refrained from imposing sectoral sanctions, instead focusing on measures against individuals and corporate entities. The main novelty in the cyber domain has been the scale and frequency of individual designations combined with criminal prosecutions: the majority of US cyber sanction measures entail individual sanctions listings, which typically involve asset

Sanctions have emerged as a potentially valuable instrument that can be used to coerce, punish or signal to 'cyber villains' the possible consequences of their actions.

Milestones in the development of the EU's cyber policy



Data: European Union

freezes and travel bans. In several of these instances, criminal indictments have also been issued to alleged perpetrators of cyberattacks. Company designations are the next most common form of US sanction, being applied in a majority of instances. Designations of government agencies in Russia, the Democratic People's Republic of Korea (DPRK) and Iran have also been issued by the US.

Looking at the trend towards a growing reliance on sanctions as a foreign policy tool also calls for the analysis of norms that were previously enforced or can be enforced in the future through the use of sanctions. Both Council Decision 2019/797 and Council Regulation (EU) 2019/796 list six types of cyberattacks against the EU member states that could result in the imposition of sanctions. These include attacks against critical infrastructure, services necessary for the maintenance of essential social and economic activities, critical state functions, the storage or processing of classified information, government emergency response teams, as well as attacks carried out against EU institutions, bodies, offices, agencies, delegations in third countries, and CSDP missions and operations. Many of these activities are also addressed through non-binding and voluntary norms promoted through various platforms discussed earlier. Their inclusion in the legal documents significantly increases the weight of those norms, violation of which would also constitute a breach of EU law.

CONCLUSIONS

Throughout this chapter, we have aimed to establish a clear link between various forms of responsible state behaviour in cyberspace and the role that sanctions play in ensuring that norms are respected. As has been demonstrated, there are currently numerous processes underway that aim to safeguard the peaceful nature of cyberspace – a sphere in which human development and growth can be promoted. However, the increasing competition between states has also turned cyberspace into a domain of conflict where existing international law, rules and norms are undermined through state practice. In most cases, irresponsible behaviour does not go hand-in-hand with accountability. Therefore, in the absence of a global norm enforcer, sanctions have emerged as a potentially valuable instrument that can be used to coerce, punish or signal to 'cyber villains' the possible consequences of their actions.

Even though the debate about sanctions as an effective tool in strengthening compliance with existing international law and respect for norms is in its early days, their signalling potential cannot be underestimated – both when it comes to decisions to target specific individuals, companies or states, and conscious choices to do nothing. Such decisions are very likely to be subjected to intense public scrutiny. It is critical, therefore, that the message that is being sent is equally clear and communicated to all potential stakeholders. This implies, for instance, that decisions about listings should provide a clear reference to laws that have been contravened or provide an explanation of which concrete norms of responsible behaviour have been violated.

CHAPTER 3

SPACE EXPLORATION

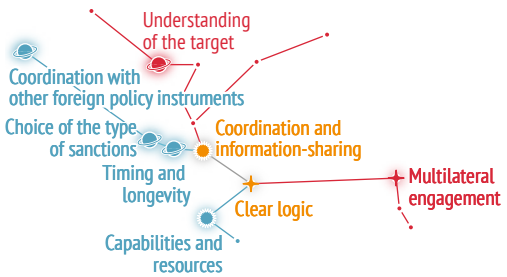
Mapping the EU's cyber sanctions regime

INTRODUCTION

Cyber sanctions – traditional measures (e.g. travel bans, asset freezes) used to deter, constrain and penalise malicious activities occurring in cyberspace – have recently emerged as a concrete mechanism to rectify the challenge of enforcement inherent to the voluntary and non-binding nature of norms in cyberspace. This has raised questions related to the application of existing international law in cyberspace. The resulting legal complexity has led to a situation where despite the expanding and deepening discussion about responsible state behaviour – expressed in numerous speeches and declarations by senior policymakers – little change has taken place in states' practice. Cyber sanctions, due to the way in which they directly affect their targets' ability to travel freely, do business or to obtain education in other parts of the world, have emerged as a potential plausible solution to the problems of enforcement and norms compliance.

The EU cyber sanctions regime, established on the basis of Council Decision 2019/797 and Council Regulation (EU) 2019/796, is the second such regime in the world. That implies that there is not much guidance regarding the practical implementation of this regime. While the elements put in place by the Decision and Regulation establish the foundations of the cyber sanctions regime, there are still many questions concerning how this new tool will be deployed in the future.[1] In that sense, with the adoption of the new thematic cyber sanctions regime the EU is entering the uncharted waters of the 'cyber galaxy'. Despite some resemblance to other thematic regimes adopted by the EU in the past and lessons drawn from the Union's experience with previous sanctions regimes, the implementation of the cyber sanctions regime will in some respects resemble the odyssey of the first space travellers. The novelty of this approach also implies that some of its underpinning concepts and principles require more extensive introduction to a broader audience. The aim of this chapter is therefore to address the following questions: what is the scope of the new regime? What are the concrete

Constellation of issues in this chapter



1 The Annex to the Decision where listed entities and individuals will be indicated remains empty (as of October 2019).

solutions adopted with regard to measures, designations and evidence? Finally, how does the cyber sanctions regime address the question of coordination with other international regimes and actors?

SCOPE OF THE REGIME

The EU's cyber sanctions regime adopted in May 2019 is one of the three thematic sanctions regimes in the EU – in addition to sanctions to combat terrorism, human rights violations, and against the proliferation and use of chemical weapons. It applies to 'cyber-attacks with a significant effect, including attempted cyber-attacks with potentially significant effect, which constitute an external threat to the Union or its Member States' (Article 1 of the Council Decision). The choice of a thematic regime resulted, *inter alia*, from the fact that the scope of the existing country-specific sanctions regimes does not cover cyber operations, even though future expansion cannot be ruled out. Such a solution might be particularly relevant to countries that have resorted to cyber operations as a means to evade the heavy burden of the sanction regimes already in place. For instance, it has been widely reported that North Korea has been responsible for multiple attacks against financial institutions and ransomware operations aimed to provide the regime with additional financial resources, when economic pressure on the country has been ratcheted up by sanctions. In such cases, where the cooperation of a government in bringing the responsible individuals to justice cannot be expected, reliance on country-specific or sectoral sanctions might be the only option. Such an approach is currently avoided but might garner support as capacities and confidence to attribute malicious cyber activities and operations increase. Nonetheless, in light of potential controversies and political costs associated with the attribution of responsibility to state actors, the thematic cyber regime put in place by the EU responds to the fact that malicious cyber activities are currently attributed to

Three types of EU sanctions

The European Union has extensive experience in the design and application of sanctions and currently has more sanctions regimes in place than either the US or the UN. EU sanctions are of three main types.*

UN-mandated sanctions: authorised by the UN Security Council (UNSC), through formal, legally-binding UN resolutions adopted under Chapter VII of the UN Charter. About one sixth of the EU's sanctions are of this kind (i.e. implemented without supplemental measures).

Supplementary sanctions: autonomous (or unilateral) measures that are adopted by the EU over and above UN-mandated sanctions. These are often justified with reference to the wording of UNSC resolutions urging member states to 'exercise vigilance' or to take additional measures recommended in UN resolutions. About a quarter of the EU's sanctions are of this type.

Autonomous sanctions: imposed in the absence of UN action. These are common in cases where the UNSC has been unable to reach agreement, typically due to opposition by, or the behaviour of, a permanent (non-elected) member or one of its close allies. Over half of the EU's current sanctions fit this latter category, and it is a type of sanction that appears to be increasingly used by the EU. Examples include EU sanctions against Russia, Syria and in relation to chemical weapons abuses. Unless mandated by the UN, any EU restrictive measures imposed in response to cyber-attacks and human rights abuses would also fall under this category.

* Thomas Biersteker & Clara Portela, "EU Sanctions in Context: Three Types", *Brief no. 26*, European Union Institute for Security Studies (EUISS), July 15, 2015, https://www.iss.europa.eu/content/eu-sanctions-context-three-types

non-state actors or individuals or entities which are not necessarily linked to the states who will be the subjects of the listings.

Establishing a sanctions regime requires a sufficiently clear definition of the scope of activities that might trigger the imposition of sanctions. Council Decision 2019/797 and Council Regulation 2019/796 define the scope of the proposed regime in Article 1. First and foremost, the cyber sanctions regime applies to attacks constituting an **external threat**, meaning, *inter alia*, cyberattacks that (i) originate, or are carried out, from outside the Union; (ii) use infrastructure outside the Union; (iii) are carried out by any natural or legal person, entity or body established or operating outside the Union; or (iv) are carried out with the support, at the direction or under the control of any natural or legal person, entity or body operating outside the Union. Consequently, the proposed regime applies also to cyberattacks within the territory of the EU as long as there is an external dimension to the cyberattack (e.g. the individual who carried out an attack is operating under the direction of a foreign government). Where there is no external dimension to a cyberattack, the perpetrator is subjected to law enforcement actions by the respective authorities.

The overall difficulty in assessing the cost of a cyber-attack highlights the primarily political nature of sanctions as a foreign policy instrument.

At the same time, sanctions as a CFSP instrument respond to situations which threaten the security or foreign policy interests of the Union or its member states, in accordance with Article 21(2) TEU. This means that sanctions could be imposed in order to achieve one or more of the Treaty's objectives, including safeguarding the EU's values, fundamental interests, security, independence and integrity; consolidating and supporting democracy, the rule of law, human rights and the principles of international law; or preserving peace, preventing conflicts and strengthening international security, in accordance with the purposes and principles of the United Nations Charter and other main international treaties. Given that some of the EU's interests are inherently linked to the stability and security of partner countries, the EU may also decide to apply sanctions in response to cyberattacks with a significant effect against third states or international organisations. In such cases, however, the imposition of EU cyber sanctions would have to be necessary to achieve CFSP objectives as defined in Article 21 TEU.

Third, the scope of the cyber sanctions is limited to activities with a 'significant effect' related to one or more of the following intrusions: access to information systems, information system interference (e.g. hindering or interrupting their functioning), data interference (e.g. deleting, damaging, altering or suppressing data) and data interception (e.g. interception of non-public transmission to, from or within an information system). Examples of such activities constituting a threat include cyberattacks on critical infrastructure, services necessary for the maintenance of the vital functions of society, and critical state functions. The regime also covers attacks posing a threat to the Union, particularly those carried out against its institutions, bodies, offices and agencies, its delegations to third countries or to international organisations, its CSDP operations and missions and special representatives.

The above definition of scope requires further clarification with regard to two elements: what constitutes a 'significant effect' and how the new regime applies to attempted activities.

Significant effect, as defined in Article 2 of the Regulation, is assessed on the basis of several concrete criteria:

- the scope, scale, impact or severity of disruption caused, including to economic and societal activities, essential services, critical state functions, public order or public safety;
- the number of natural or legal persons, entities or bodies affected;
- the number of member states concerned;

- the amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property;
- the economic benefit gained by the perpetrator, for itself or for others;
- the amount or nature of data stolen or the scale of data breaches; or
- the nature of commercially sensitive data accessed.

However, the wording of the criteria and the non-exhaustive nature of the list points to their subjective and context-specific nature, which raises several questions about how the ultimate determination of the effect will be made by the state concerned and subsequently evaluated by other member states in the Council. In particular due to the fact that the scale of an attack and its impact will depend on the overall level of preparedness of individual member states. In that sense, the truth about the scale and significant effect is always in the eye of the beholder. For instance, the overall difficulty in assessing the cost of a cyberattack highlights the primarily political nature of sanctions as a foreign policy instrument. In addition, many of the consequences are long-term in nature and are difficult to assess through simple quantification mechanisms. The loss of customer trust is often mentioned as translating into serious financial consequences for businesses. The cost of data breaches is also different from one country to another: the cost of a data breach in the US corresponds to $8.19 million as compared to $4.78 million in Germany, $3.30 million in South Korea, or $1.35 million in Brazil.[2]

The primary focus of the proposed regime is on the effect of and the actual significant harm caused by cyber activities. However, Decision 2019/797 and Regulation 2019/796 also refer to measures in response to attempted damaging cyber activities which could have a significant effect. Decisions in this regard will be taken by the Council on a case-by-case basis. There are, however, several questions associated with any listing on the basis of 'an attempt'. First of all, it might be difficult to establish a clear link between an activity in the cyber domain and a potential attempt to cause significant harm. Given the difficulty in measuring the economic and societal impact of cyberattacks, it might be challenging to prove the significant effects of an operation that has not terminated, and to respond in a way that takes into consideration the legal principle of proportionality. The determination whether an attempt warrants a response by listing would require taking into account the broader context and circumstances surrounding the threat actor and the incident itself. This might be easier in scenarios where cyberattacks have been successfully prevented, disrupted and defended against, and hence have not resulted in significant damage, but to which the EU may still wish to respond in a decisive manner by sending a political signal. Having said this, although pre-emptive responses may play an important deterrent role, if used prematurely, such responses might end up undermining the credibility and effectiveness of the whole cyber sanctions regime.

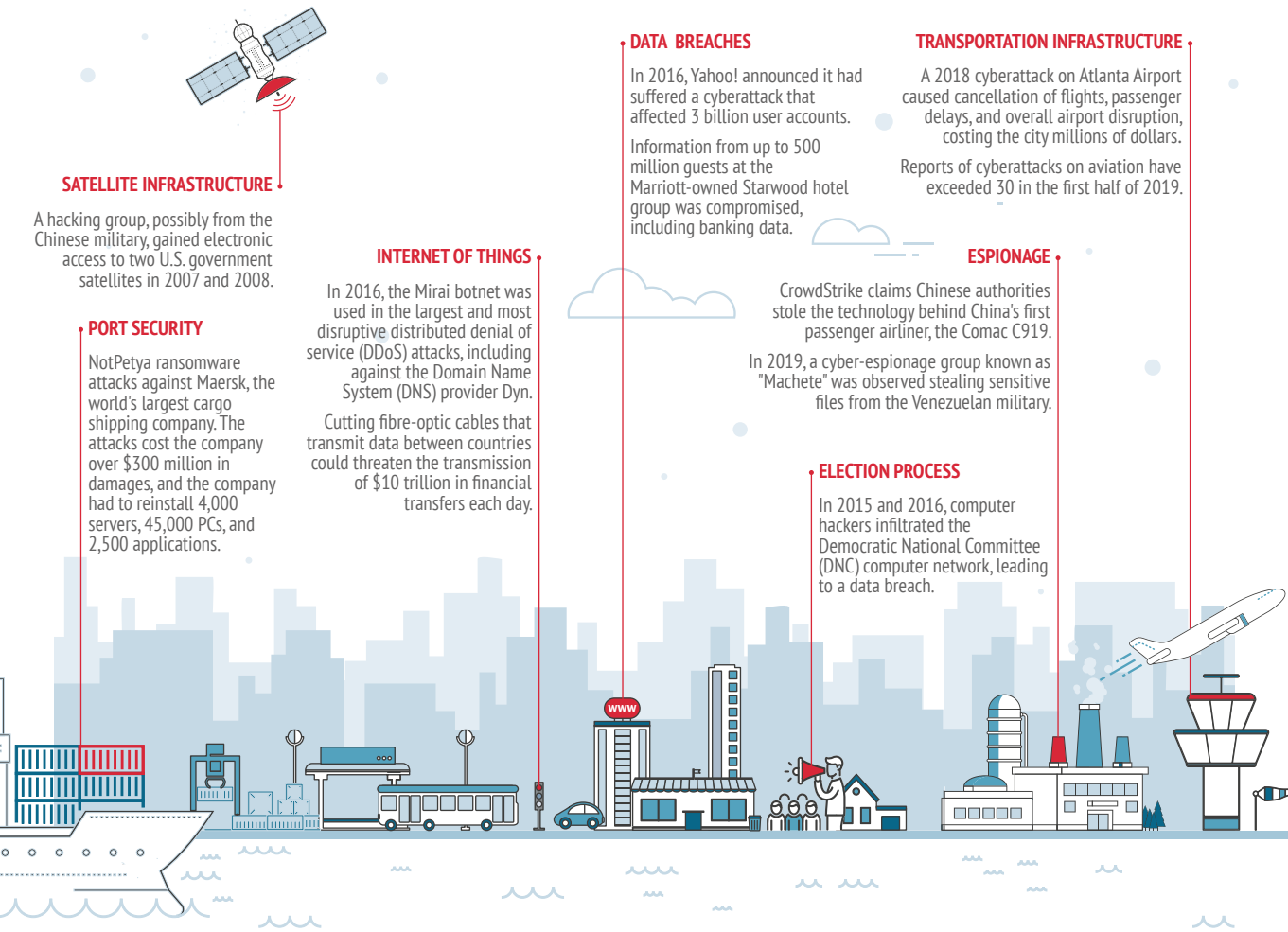
Another question worth considering is that of the link between the level of preparedness and capacities of an individual member state and the potential impact of a cyber operation targeting that member state. It is not difficult to anticipate a situation where a group of EU member states suffer significant consequences of a cyberattack due to their own negligence and failure to implement or transpose relevant EU legal frameworks and security recommendations. In addition, human error and system vulnerabilities still remain the underlying cause of a significant number of data breaches.[3] In such cases – where the target has neglected to mount appropriate network security defences – it might prove challenging to secure the solidarity of member states unwilling to pay the political price for others' mistakes. In order to ensure that the EU cyber sanctions regime becomes robust and trustworthy, the European

2 IBM Security & Ponemon Institute, *Cost of a Data Breach Report*, 2019.

3 In many case of breaches, human error is indicated as a root cause. See: Verizon, "2019 Data Breach Investigations Report", 2019, https://enterprise.verizon.com/resources/reports/dbir/

Significant impact of cyberattacks

examples of past cases



Commission, as the guardian of the Treaties, needs to ensure member states' full compliance with the already existing cybersecurity legislation (e.g. the NIS Directive) and put forward new initiatives aimed at enhancing the overall level of cyber resilience and defence across the European Union.

MEASURES, DESIGNATIONS AND EVIDENCE

The horizontal sanctions regime adopted by the EU consists of conventional sanctions measures: travels bans and/or asset freezes.[4]

4 Article 4 of the Council Decision 2019/797 and Article 3 of the Regulation 2019/796 respectively.

According to the Council Decision, member states shall take the measures necessary to prevent the entry into, or transit through, their territories of individuals who are responsible for cyberattacks or attempted cyberattacks as well as any person who provides financial, technical or material support for such activities. More specifically, according to Decision 2019/797 the provision of support encompasses involvement in the planning and preparation of and participation in, directing, assisting or encouraging such attacks, or facilitating them whether by action or omission. Furthermore, the EU's cyber sanctions regime covers measures against individuals associated with those committing or attempting to commit cyberattacks. In addition, Council Decision 2019/797 and Council Regulation 2019/796 foresee the freezing of all funds and economic resources belonging to, owned, held or controlled by individuals and entities based on similar designation criteria. In this way, whereas individuals can be the target of asset freezes and/or travel bans, entities can only be subjected to asset freezes.

The adopted cyber sanctions regime declares that the fundamental rights and the principles enshrined in the Charter of Fundamental Rights of the European Union, in particular the right to an effective remedy and a fair trial and the right to the protection of personal data, need to be fully respected when adopting a new set of sanctions. To ensure maximum legal certainty within the Union, whenever the Council decides on a listing of an individual or an entity,[5] it should communicate such decisions, including the legal and material grounds for the listing, to those concerned, either directly or through the publication of a notice. In cases where the targets of sanctions submit competing observations on the provided rationale, or where substantial new evidence is presented, the Council should review its decision and inform the addressees accordingly. Moreover, the right to effective judicial protection facilitates, *inter alia*, access to evidence substantiating the adoption of sanctions. The Court of Justice of the EU guarantees the execution of this right and provides judicial oversight of the adopted measures. The case-law of the Court demands that listings should be accompanied by an accurate, up-to-date, defendable and clear statement of legal reasoning and the necessary material information in accordance with human rights and fundamental freedoms, and the principle of proportionality.[6]

Usually listings are based on open-source information, or at least information that can be shared with the member states, the listed person and the Court. However, there might be instances where the listing will contain information or material which would harm the security of the Union, its member states, and the conduct of international relations. In such cases, the handling of information follows specific rules laid out in Chapter 7 of the Rules of Procedure of the General Court.[7] Upon requests for confidential handling of information, the Court examines the information or material provided taking into consideration the right to effective judicial protection and the security of the Union and its member states. Where the General Court decides that the produced information is relevant for the case and merits to be treated as confidential, the Court should make a reasoned order specifying the adoption of further procedures, which include the production of a non-confidential version or a non-confidential summary of the information or material enabling the target of the sanctions to make its views known. It is worth noting that even in cases of non-compliance with this requirement, the General Court can still consider

5 The Annex with listings should contain, where available, the information necessary to identify the natural or legal persons, entities or bodies concerned. In the case of natural persons: names and aliases; date and place of birth; nationality; passport and identity card numbers; gender; address, if known; and function or profession. With regard to legal persons, entities or bodies: names, place and date of registration, registration number and place of business.

6 In the Kadi II case (C-584/10P) the Court made a number of important statements regarding the review (listings need to be taken on a sufficiently solid factual basis, which entails a verification of the factual allegations whereby at least one of the reasons provided should support the listing), the information or evidence substantiating the reasons for listing (the information or evidence produced should support the reasons relied on against the person concerned), handing the confidential information (it is for the Court to determine whether the reasons relied on by that authority as grounds to preclude that disclosure were founded).

7 It is worth noting that this procedure has not been used by the Court so far.

the confidential information in forming its judgment. The reliance on open-source information and sources is one of the ways to avoid any potential complications with confidentiality and security concerns.

Finally, the cyber sanctions regime needs to provide for a transparent and effective de-listing procedure in order to ensure the credibility and legitimacy of restrictive measures. De-listing is appropriate wherever the criteria for the listing are no longer met, including evidence of mistaken listing, a relevant subsequent change in facts, or the emergence of new evidence.[8] In addition to requests for de-listing, such decisions can be also taken following a regular review (i.e. at least every 12 months in case of the Council Regulation 2019/796 and regular review for the Decision 2019/797). De-listing plays a particularly important role in the cyber context given that it is nearly impossible to obtain absolute certainty about the perpetrators of an attack or an attempted attack. Additional complication may result from specific cyber-scenarios, such as the use of 'false flag' attacks and the planting of evidence pointing to another actor, which, if taken into account, would result in an unjust listing. Listed persons and entities may also initiate proceedings against sanctions addressed to them; however, even in the event of a favourable judgment of the General Court, such decisions do not always immediately enter into force. The time gap between the judgment and publication gives relevant EU institutions the opportunity to remedy the infringement by adopting, if appropriate, new restrictive measures with respect to the persons and entities concerned and *de facto* for ensuring the continuance of the sanctions.

De-listing plays a particularly important role in the cyber context given that it is nearly impossible to obtain absolute certainty about the perpetrators of an attack or an attempted attack.

While recognising the Council's broad discretion in establishing the designation criteria, such an extensive approach may eventually raise a number of challenges. The logic of applying sanctions is to respond to harms done in equal measure, establish or reinforce norms of behaviour in cyberspace, and provide deterrence against future attacks. The determination of the particular type of sanctions applied is based on the degree of confidence of attribution for the attack and strength of evidence used for listings as well as taking into account the principle of proportionality. At the outset, there needs to be a process to develop a reasonable basis for the determination of attribution of the source of a cyberattack which then leads to a listing. In the case of US justification for countermeasures applied to North Korea over the massive hacking operation against SONY Pictures Entertainment, there were both technical similarities aligned with past patterns of cyberattacks emanating from the country, and the DPRK's politically-motivated response to the satirical characterisation of the regime in a feature film. Attribution therefore entails both technical information and political analysis. In addition to attribution, responses to cyberattacks need to be founded upon a legal determination of proportionality. This is inherently present in the application of all international sanctions. Ultimately, the individuals listed under the cyber sanctions regime should be clearly linked to the specific malicious activity, or hold responsibilities in state agencies that engage in cyberattacks.

8 Council of the European Union, *Restrictive Measures (Sanctions) – Update of the EU Best Practices for the Effective Implementation of Restrictive Measures*, Brussels, 4 May 2018.

Towards the EU's cyber sanctions regime

key developments

2004

The EU recognises that the use of restrictive measures needs to be continuously adapted to reflect changes in the security environment.

2013

Directive on attacks against information systems identifies the emerging threat from malicious cyber activities and the need for effective criminal sanctions.

2015

Council conclusions on cyber diplomacy recognise that the mitigation of cybersecurity threats, conflict prevention and greater stability in international relations require a diplomatic approach alongside a legal approach. In particular, a joint EU diplomatic response should seek to impose consequences on malicious actors in cyberspace.

2017

The EU Cyber Diplomacy Toolbox (CDT) recognises that an enhanced response is needed to address the increased ability and willingness of state and non-state actors to pursue their objectives by undertaking malicious activities. It identifies a range of tools than can be employed depending on the severity of the situation. The same year the PSC adopts the Implementing Guidelines for the Toolbox.

The Joint Communication on resilience, deterrence and defence mentions the CDT as a mechanism for creating effective cyber deterrence. The document reaffirms that the CDT constitutes an important step in the development of signalling and reactive capacities at EU and member states level.

2018

The Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats calls on member states to continue their work on the practical use of the Toolbox and to formulate a political response to cyber operations.

The Council conclusions of 16 April 2018 on malicious cyber activities underline that the CDT sets out measures, including restrictive measures, which can be used to prevent and respond to malicious cyber activities.

In June, the European Council Conclusions stress 'the need to strengthen capabilities against cybersecurity threats from outside of the EU' and ask 'the institutions and Member States to implement measures referred to in the Joint Communication, including the work on attribution of cyber-attacks and the practical use of the cyber diplomacy toolbox'.

In September, the Horizontal Working Party on Cyber Issues (HWP) holds the first exchange of views on the legal framework for restrictive measures and requests the EEAS to produce a non-paper outlining the possibilities for 'cyber sanctions'.

In October, the European Council adopts conclusions which call for advancing the work on the capacity to respond to and deter cyberattacks through EU restrictive measures.

In November, the EEAS presents a non-paper, followed by several rounds of discussions in the HWP on the basis of comments provided by the member states.

2019

The final version of the non-paper is adopted in February, opening the way for the formal process in the Council.

On 17 May 2019, the Council adopts the Council decision and regulation on restrictive measures to counter cyberattacks threatening the Union and its member states, including cyberattacks against third states or international organisations where restricted measures are considered necessary to achieve the objectives of the Common Foreign and Security Policy (CFSP).

Data: European Union

COORDINATION WITH OTHER INTERNATIONAL REGIMES

EU sanctions typically overlap with sanctions applied by other actors, most notably the UN and the US.[9] In practice, other EU allies, such as Canada, Australia, Japan, South Korea and New Zealand, also tend to follow the examples set by the US and EU.

The EU also invites a range of European and partner countries to align with its sanctions. These include EEA countries (Norway, Iceland, Liechtenstein), accession countries (Turkey, Montenegro, Albania) and those in partnership agreements or other forms of strategic relationships, such as Ukraine, Moldova and Georgia. Switzerland also matches its unilateral sanctions practice with about half of the EU's measures, while exercising autonomy in deciding which ones to implement.[10] Once the EU has made its decision, neighbouring European countries are invited to join in implementing similar measures. Little to no consultation takes place, however, and these countries play no role in the decision-making process. Alignment is typically a political decision and most partner countries are not under any legal obligation to mirror EU measures (although in the case of candidate countries, alignment forms part of the *acquis* linked to their candidacy progress).[11]

Alignment is typically a political decision and most partner countries are not under any legal obligation to mirror EU measures

When combined with US measures already in place, the weight of overlapping sanctions could act as a force multiplier, both in terms of the possible impact of the measures, as well as in terms of the symbolic weight implicit in a concerted body of nations working together to express their disapproval of a given act perpetrated in cyberspace. The overlapping of sanctions regimes, however, also presents challenges in terms of how these measures could be collectively monitored, evaluated and coordinated: something that is not currently done through any existing, formalised arrangement, other than in some *ad-hoc* groupings and task forces relating to a number of specific sanctions regimes.

The cyber sanctions sphere has already been marked by a number of *ad-hoc* groupings taking the lead on joint attributions. For example, there was a joint attribution between the 'Five Eyes' countries (Australia, Canada, New Zealand, UK, US) in response to the May 2017 Wannacry ransomware attack, which targeted computers running Microsoft Windows by encrypting data and asking for cryptocurrency ransom payments. The EU, NATO allies and France issued statements in support of the UK and Netherlands in relation to the cyberattacks on the OPCW in the Netherlands in October 2018, which was linked to the investigation of the Salisbury chemical weapons attack in the UK. Such *ad-hoc* groupings are common in sanctions formulation more widely, both within the EU and between the EU and other major sanctioning and diplomatic powers, whereby core countries have worked together informally to

9 Indeed, one researcher asks whether the development of a cyber sanctions regime in the EU 'has something to do with Washington's desire to see its European partners adopt legal instruments that permit the easy transfer of its own listings'. See Clara Portela, "The Spread of Horizontal Sanctions", *CEPS Commentary*, Centre for European Policy Studies (CEPS), Brussels, 2019.

10 Embassy of Switzerland in the United Kingdom, written evidence, Select Committee on the European Union, External Affairs Sub-Committee, 'Swiss Sanctions Policy', September 19, 2017, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-external-affairs-subcommittee/brexit-sanctions-policy/written/70458.pdf.

11 Erica Moret and Fabrice Pothier, "Sanctions After Brexit", *Survival*, vol. 60, no. 2, (2018): pp. 179-200, https://doi.org/10.1080/00396338.2018.1448585.

reach a decision on sanctions before bringing it before the wider group.[12]

The emerging EU cyber sanctions regime could be combined with other unilateral and multilateral sanctions frameworks, and there is a possibility of potential synergies stemming from joint designations from different countries and regional or international organisations. This has been the case of effective sanctions regimes in the past, such as the combined effects of UN, US and EU measures applied against Iran between 2006 and the signing of the Joint Comprehensive Plan of Action (JCPOA) in 2015. The UN Security Council has yet to denote cyber operations as a threat to international peace and security, even though the idea has been discussed informally for years. So far, the UN has engaged in efforts to close down or degrade particular websites associated with support for the commission of acts of terrorism. However, the link between the UN's own sanction regimes and cyberattacks is increasingly difficult to deny. According to one UN panel of experts report, Kim Jong-un's government has generated an estimated $2 billion using 'widespread and increasingly sophisticated' cyberattacks to steal from banks and cryptocurrency exchanges.[13] These attacks were mostly launched by cyber operatives working under the direction of the Reconnaissance General Bureau – a North Korean intelligence agency that manages the state's clandestine operations.

CONCLUSIONS

The purpose of this chapter has been to provide a general overview of the cyber sanctions framework adopted by the EU. Three features of this regime are important to highlight. First, the scope of the regime is clearly defined while remaining relatively broad. Such an approach seems to be justified given the rapid pace of technological development and the complexity of the security challenges emanating from cyberspace. The challenge though remains projecting clearly the purpose of the sanctions: *coercion*, *constraint* or *signalling*. Second, the concrete measures foreseen by the regime include travels bans and/or asset freezes. That does not imply that the EU and its member states cannot rely on other foreign and security policy instruments. Quite on the contrary: sanctions need to be used as part of a holistic approach to external relations. That implies that not using them is also a matter of political choice and reflects a broader political assessment. Such decisions, however, will need to be accompanied in the future by an adequate strategic communication strategy. Finally, the cyber sanctions regime can also be used for cyber activities targeting the EU's allies and partners – an important aspect given that the EU's engagement with and interests in third countries are increasingly challenged through cyber means. This of course does not imply that such measures will be applied automatically upon request. There are currently no listings under the adopted regime which highlights some open questions that will need to be addressed in the coming months to make this regime robust and effective. The following chapters of this *Chaillot Paper* do not discuss the EU's sanctions regime *per se* but some of the dilemmas that will emerge in the discussions, with more detailed work still required on attribution, evidentiary standards, international law concepts, cooperation with private sector actors and the possible unintended consequences of the regime.

12 Erica Moret, "Effective Minilateralism for the EU: What, When and How", *EUISS Brief* no. 17, June 3, 2016, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_17_Minilateralism.pdf.

13 United Nations, "Midterm Report of the Panel of Experts submitted pursuant to resolution 2464", August 30, 2019, https://undocs.org/S/2019/691.

CHAPTER 4

MISSION CONTROLS

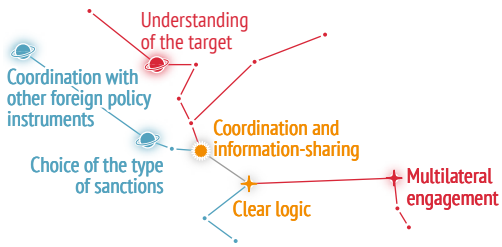
Sanctions under international law

INTRODUCTION

When astronauts venture outside of a spaceship, they wear specially constructed pressurised suits that protect them from the harsh environment of space and maintain constant communication with the crew and mission control centre. International law performs both the function of a pressurised suit and the mission control centre when it comes to cyberspace. The conditions in cyberspace are equally as harsh as those prevailing in the space over 100 kilometres above our heads: in addition to 'cyber debris', state and non-state actors conduct their own operations, which makes the cyber environment quite unpredictable. International law reduces this unpredictability by providing clear indications of what is and what is not permitted in cyberspace, and applies to all state actors. In the context of sanctions, international law offers guidance on one important question: when are sanctions against certain activities in cyberspace legal as an instrument of foreign policy? In that sense, international law provides protection to those states who might be the target of an unjustified and unsubstantiated response from another state party. Due to their targeted nature, the measures applied as part of the EU sanctions regime are qualified as measures of retorsion (unfriendly but legal acts). The threshold for sectoral or country-specific cyber sanctions (countermeasures) would be higher and subjected to a different level of evidentiary scrutiny.

International law and, in particular, the Charter of the United Nations are the backbone of international relations and crucial for maintaining international peace and security. Yet, it may be wondered whether a state will consider international law as a suitable framework within which to address a massive cyber operation meddling with its election process, shutting down its electricity network or blowing up an industrial facility on its territory. Even though many countries have invested heavily in developing their own defensive and offensive capabilities to prevent, prepare for and respond to malicious cyber intrusions, international law gives the state victims recourse to judicial measures to compel the wrongdoing state to fulfil its obligations, but also extrajudicial ones such as measures of retorsion, countermeasures and self-defence. However, under existing international law, both perpetrators and victims have certain obligations and rules to comply with or else they must face consequences. For these reasons, it is important to assess the

Constellation of issues in this chapter



lawfulness of sanctions in international law[1] and their potential effect as compared to other policy instruments available. Due to the fact that sanctions might have a certain escalatory effect, their impact should be carefully assessed. In other words, one of the key questions when contemplating the adoption of new sanctions should be: are the sanctioning states entitled by international law to adopt sanctions against the responsible state and non-state actors? The important point to make at the outset of this chapter is that international law addresses the relations between states only and therefore measures such as targeted sanctions against individuals or entities – which under international law can be characterised as measures of retorsion – are not necessarily subjected to the same criteria as sanctions against states, which would constitute and enable countermeasures. The following sections discuss the general options available to states when their rights are violated and present the options for possible responses, including through cyber sanctions.

CYBER SANCTIONS AND SELF-HELP IN INTERNATIONAL LAW

When faced with cyberattacks and in the absence of concrete actions undertaken on the basis of existing international instruments – including by the UN Security Council – international law allows, depending on the circumstances, three different forms of measures of self-help: **measures of retorsion**, **countermeasures** and **self-defence**, the two latter being otherwise illegal.[2] Measures of retorsion are acts that are not unlawful. They are generally unfriendly acts taken in response to a prior unfriendly act. Countermeasures are acts that would normally be unlawful, but their unlawfulness is precluded by the unlawfulness of the act to which they were initially responding. For instance, the victim state of an unlawful state-sponsored cyber operation can respond also by launching a cyber operation against the responsible state. The unlawfulness of this cyber operation will be precluded, as it constitutes a countermeasure.[3]

Self-defence is the most well-known and the ultimate form of self-help. The customary right to self-defence enshrined in Article 51 of the United Nations Charter is the principal exception to the prohibition against the use of force. A state targeted by a cyber operation constituting an armed attack has the right to resort to self-defence, using either cyber operations or other forms of force such as kinetic force.[4] However, there is no agreed definition of armed attack in cyberspace. The International Court of Justice (ICJ) interprets armed attack as 'the most grave form of the use of force'.[5] Accordingly, it is generally asserted that only cyber operations causing death, injuries or physical damage and reaching a certain level of intensity may be considered as armed attacks.

The right of self-defence is the only circumstance under which a victim state is authorised by international law to use force, including

1 See, for instance: Pierre-Emmanuel Dupont, "Countermeasures and Collective Security: The Case of the EU Sanctions Against Iran", *Journal of Conflict and Security Law*, vol. 17 (2012): p.301.

2 For a more developed analysis, see: François Delerue, *Cyber Operations and International Law* (Cambridge: Cambridge University Press, 2019), Chapter 10.

3 For a countermeasure to be considered lawful, it should: (i) respond to an unlawful act perpetrated by the responsible state; (ii) follow the request for the responsible state to cease its act; (iii) be notified by the reacting state prior to launching countermeasures, unless the countermeasures are urgent; (iv) be proportionate; (v) end as soon as the violation of international law has ceased.

4 The right of self-defence requires that three conditions be met: (i) the action must be undertaken in response to an armed attack; (ii) the use of force must be necessary and proportionate; (iii) the state undertaking the action must report it to the UN Security Council. A state must cease its resort to self-defence when the Security Council has taken "measures necessary to maintain international peace and security" (Article 51.)

5 International Court of Justice, "Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)", (Merits), *ICJ Reports*, no. 14, 1986, p. 119, para 228.para 191.

kinetic force, against cyber operations. It is important to note that countermeasures and measures adopted in self-defence must meet the two cumulative criteria of necessity and proportionality. There are also two important differences between countermeasures and self-defence. Firstly, self-defence may be exercised individually or collectively. There are two conditions for collective self-defence: the victim state must consider itself the victim of an armed attack, and the third state should intervene at the request of the victim state. Conversely, countermeasures can be adopted only by the injured state, there is no right to take collective countermeasures.[6] It should be noted, however, that some states and scholars advocate the existence of a right of collective countermeasures pursuant to the law of state responsibility.[7] Secondly, self-defence may be invoked only to coerce the wrongdoing state to cease its wrongful act, while countermeasures may be used to obtain both the cessation of the act and the reparation of the resulting injury.

In some circumstances, the wrongfulness of the reaction of a state to a cyber operation, which is not justified as a countermeasure or measure of self-defence, may be excused by another circumstance precluding wrongfulness, such as *force majeure*, distress, consent or necessity. For instance, if the adopted response constitutes the only means for a state to safeguard an essential interest against a grave and imminent peril, its wrongfulness would be precluded by the plea of necessity.

International law performs both the function of a pressurised suit and the mission control centre when it comes to cyberspace.

CYBER OPERATIONS AND STATE RESPONSIBILITY

One of the main aspects in the discussion about responsible behaviour, as mentioned earlier, is promoting more compliance with existing international law and norms by holding the responsible state accountable for a cyberattack. The state injured by a cyber operation may invoke the responsibility of other states in relation to this cyber operation in two distinct circumstances. First, it may be entitled to invoke the responsibility of the sponsoring state and to seek reparations for the damage caused. Second, it may be entitled to invoke the responsibility of a state that let its territory be used for the perpetration of the cyber operation.[8] While in some cases linking a state to an operation might be possible, most of the time states act through proxies – individuals or other entities – which makes establishing such a link more complicated.

How to deal with the challenge posed by individuals and corporate entities is a complex question. From the international law perspective, establishing such a link implies the responsibility of a state on behalf of which or under the control of which those actors have acted. However, in the context of targeted sanctions that link is not automatic as the listing itself is not the equivalent of

6 Most of the time we are talking about retorsion, not countermeasures, and the simple fact that states are part of an alliance does not mean that they conduct collective countermeasures.

7 At the 2019 CyCon Conference, the Estonian President stated that "[a]mong other options for collective response, Estonia is furthering the position that states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation": President of Estonia, "President of the Republic at the Opening of CyCon 2019", May 2019, https://president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/ ; See an analysis of this position in: Michael N. Schmitt, "Estonia Speaks Out on Key Rules for Cyberspace", *Just Security*, June 10, 2019, https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/

8 See: François Delerue, "International Law in Cyberspace Matters: This Is How and Why", *Ideas in Focus*, EU Cyber Direct, May 16, 2019, https://eucyberdirect.eu/content_research/international-law-in-cyberspace-matters-this-is-how-and-why/; The two editions of the *Tallinn Manual* published in 2013 and 2017 offer a good overview on the applicability and application of the norms of international law to cyber operations: Michael N Schmitt (ed), *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013); Michael N Schmitt and Liis Vihul (eds), *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).

attribution, as understood by international law. Such a distinction, while clear for policymakers and lawyers, may not be that obvious to make for the public or other countries which might interpret such a move simply as avoiding political confrontation.

While the criteria for listings of individuals and corporate entities are decided by the Council of the European Union, under international law, the responsibility of a state for a cyber operation may be invoked if two cumulative criteria are met: the cyber operation is attributable to that state and constitutes an internationally wrongful act. To be attributable to that state, the operation must have been carried out by one of its organs or by another actor acting on its behalf. A cyber operation attributable to a state may constitute an internationally wrongful act if it violates a norm of international law. Indeed, the development of cyber capabilities and cyber operations is not wrongful *per se* but their use may violate specific norms of international law, such as the territorial sovereignty of a state, the prohibition of intervention, the prohibition of the use or threat of force as well as of human rights.

Alternatively, in some cases, even if a cyber operation is not attributed to a state, that state may be still held responsible according to the principle of due diligence.[9] This principle imposes a duty on states not to allow their territory to be used for the launch or the transit of cyber operations targeting another state. The principle of due diligence is an obligation of conduct and not one of result. A state will incur responsibility not because it did not achieve the expected result but because it manifestly failed to take the necessary but feasible measures to prevent the act from happening despite being under an obligation to do so. For instance, a state that has taken no steps to mitigate an attack originating from its territory may be still held accountable under international law. The attribution of the act does not matter; it can be perpetrated by a state or a non-state actor. In that perspective, due diligence may constitute an interesting palliative to the problem of attribution.

It is necessary to recall that international law imposes an obligation on states to settle their international disputes by peaceful means. The consequences of the invocation of the responsibility of the wrongdoing state are twofold. The responsible state bears the obligation to cease its wrongful act and is obliged to make full reparation for the damage resulting from its wrongful act. The victim state should first ask the responsible state to comply with its obligations. If the responsible state does not comply, the injured state may have recourse to judicial and extrajudicial processes, such as the UN Security Council or the International Court of Justice, to coerce the wrongdoing state to comply with its obligations. However, a central, compulsory judicial and enforcement mechanism may not always be available. Therefore, self-help measures constitute an important tool for the enforcement of international law. The victim state of an unlawful cyber operation may have recourse to extrajudicial measures to compel the wrongdoing state to fulfil its obligations, namely measures of retorsion, countermeasures and self-defence.

SANCTIONS AND STATE PRACTICE

Academic literature and state practice over the past few years have been disproportionately dominated by the focus on self-defence. For instance, following the large-scale Distributed Denial of Service (DDoS) attacks it experienced in 2007, Estonia initially explored the possibility of invoking Article 5 of the North Atlantic Treaty, thus treating the cyber operations as an armed attack, triggering the right of individual or collective self-defence. However, the vast

9 See: Karine Bannelier-Christakis, « Obligations de diligence dans le cyberespace : qui a peur de la cyber-diligence? » *Revue belge de droit international*, 2017, p. 612; Joanna Kulesza, *Due Diligence in International Law* (Leiden: Brill & Martinus Nijhoff Publishers, 2016).

majority of cyber operations do not qualify as a use of force[10] and, *a fortiori*, an armed attack. Consequently, in such cases, the injured state cannot invoke the right to self-defence.

The conclusion that most cyber operations fall short of an armed attack has led some scholars to alternatively consider the possibility of measures of retorsion and countermeasures as a response to state-sponsored cyber operations. However, countermeasures could also be considered as the primary and preferred form of self-help against cyber operations. This would then mean that self-defence is only considered in exceptional cases. The argument is not that self-defence should be totally off the table as a possibility, but it should not constitute a default approach and form of remedy. Consequently, measures of retorsion (such as targeted sanctions, expulsions of diplomats) and countermeasures (such as sectoral sanctions) constitute a valid alternative in response to an internationally wrongful cyber operation.

International law reduces this unpredictability by providing clear indications of what is and what is not permitted in cyberspace.

Measures of retorsion

States may always have recourse to measures of retorsion, that is to say lawful but unfriendly measures. By adopting measures of retorsion, a state expresses its disagreement with the activities of another state within the limits of the law. Such measures may take a wide variety of forms, including: severance or interruption of diplomatic relations or of other forms of contact; expulsion of diplomats, journalists or other citizens of the targeted states; travel restrictions; restrictive control of aliens; reduction or interruption of economic aid programmes; various forms of economic and commercial restrictions; and trade embargoes.[11] Traditionally, and notably outside of the cyber realm, sanctions generally take the form of measures targeting a state, individuals or corporate entities. They may take a great variety of forms, such as travel restrictions, the freezing of assets, restrictions on importation or exportation of certain products, restriction on the use of certain products, and finally restrictions in the field of academic and research cooperation. Most of these measures are lawful under general international law and thus constitute measures of retorsion rather than countermeasures. In numerous circumstances, however, they may constitute a breach of specific regimes of international law, such as the law of the World Trade Organisation (WTO)[12] or bilateral agreements, and thus constitute unlawful acts. In that sense, the demarcation line between countermeasures and measures of retorsion may sometimes be difficult to draw. This distinction has important implications for those imposing such measures, in particular with regard to the need for notification and evidentiary standards.

Countermeasures

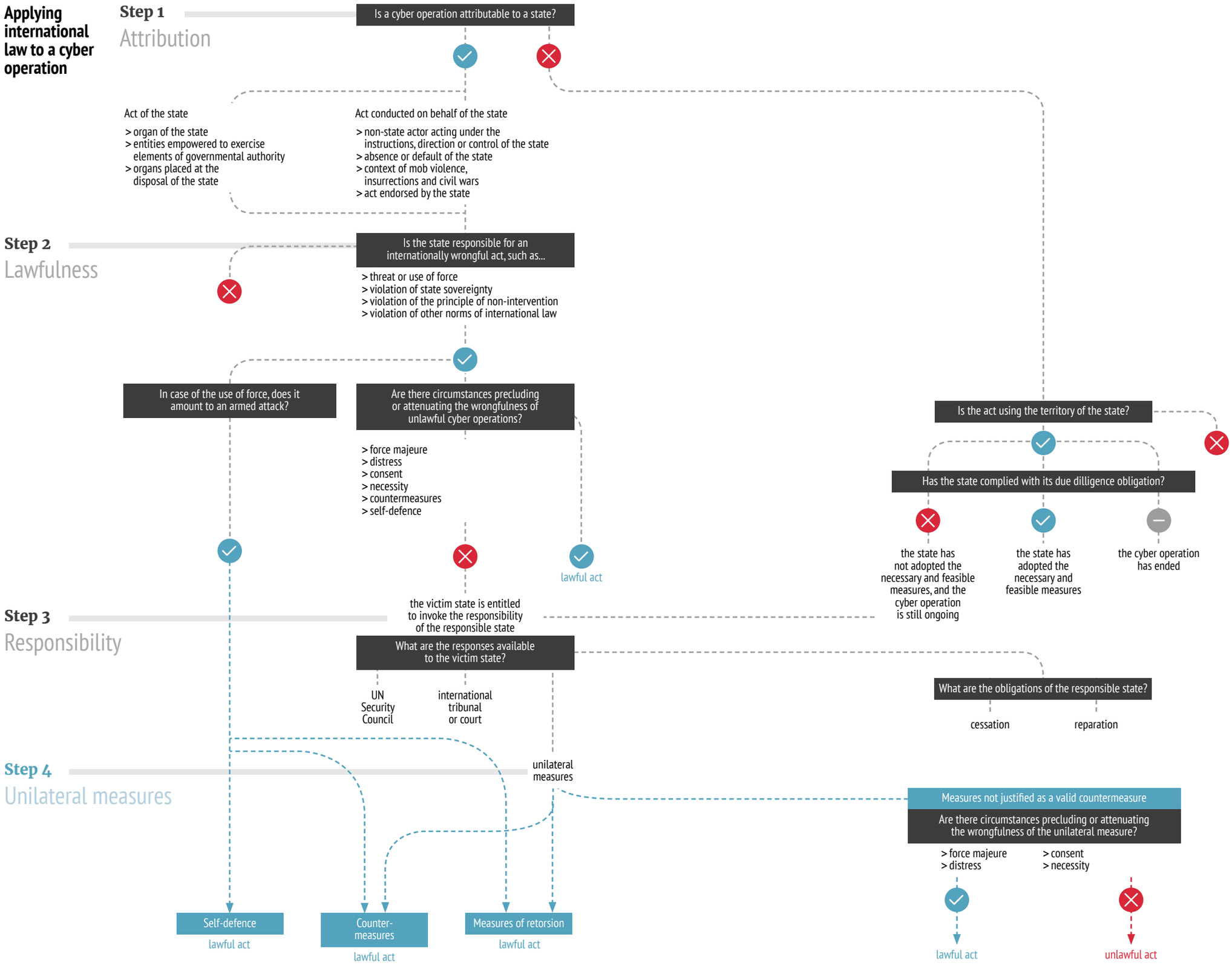
The development of cyberspace offers a wide range of new forms of countermeasures. Among these, the most straightforward category consists of what we may call counter-cyber operations. The state injured by an internationally wrongful act, being either a cyber operation or another type of act, may choose to resort to cyber operations as countermeasures. For instance, a state targeted by a large-scale DDoS

10 There is no agreed definition of a use of force in cyberspace. However, it is generally asserted that only cyber operations causing death, injuries or physical damage wold qualify as uses of force.

11 International Law Commission, "Commentary to the Articles on State Responsibility", 2001, p. 2; *Yearbook of the International Law Commission* (Part II), pp. 31, 128; Malcolm N Shaw, *International Law* (7th edn, Cambridge: Cambridge University Press, 2014), p. 818; Alain Pellet *et al*, *Droit international public* (LGDJ, 2009), no. 573, pp. 1057–58.

12 Note however, the exceptions allowed by the WTO in cases of national security (Article XXI of the General Agreement on Tariffs and Trade). This is what prevented the Russians from challenging the US and EU in the appellate body.

Applying international law to a cyber operation



Data: EU Cyber Direct, 2019

attack sponsored by a state and violating its sovereignty, may decide to resort to a proportionate cyber operation against the Command and Control server used for this DDoS attack on the territory of the wrongdoing state. In such a case, the wrongfulness of the cyber operation against the Command and Control server would be precluded as it constitutes a valid form of countermeasures.

Countermeasures in the cyber realm may also take the form of supporting non-state actors acting against the wrongdoing state – for instance, by allowing them to use the ICT infrastructure located on the territory of the state adopting the countermeasure. Such action may constitute a violation of the obligation of due diligence of that state, but its wrongfulness could be precluded if adopted as a form of countermeasure. The support to non-state actors could also take the form of the provision of exploits or tools necessary to conduct a cyber operation against the wrongdoing state. In the *Nicaragua* case, the ICJ ruled that the arming and training of armed opposition forces and the mere supply of funds could amount to an unlawful intervention, and that the former could also constitute a use of force.[13]

The evolution from traditional forms of countermeasures to those arising with the development of ICTs also challenges their implementation and the repartition of competences within states. Traditional countermeasures would typically be implemented by the institutions in charge of economic matters as well as the ministry of foreign affairs. Conversely, cyber-related countermeasures are to be implemented by institutions in charge of defence and national security in conjunction with the ministry of foreign affairs. This shift with regard to the implementation of sanctions and unilateral measures may appear particularly challenging for states since it may request some adaptation to their traditional policy functioning.

To date, no state has ever publicly framed its response within the international legal mechanism of countermeasures or invoked the right of self-defence in response to cyber operations. The example of the US responses to the hacking of the Democratic National Committee (DNC) during the 2016 US presidential elections is illustrative. On 7 October 2016, the Department of Homeland Security and the Office of the Director of National Intelligence published a joint report affirming that the Russian government was responsible for various hacks and the online publication of Democratic Party documents.[14] On 10 October 2016, the White House announced that the US government would adopt a proportionate response and, on 29 December 2016, it launched new sanctions against Russia and certain individuals. President Obama also expelled 35 Russian diplomats from the country, who left US territory on 1 January 2017.

It must be highlighted, however, that the US has also been accused of resorting to extrajudicial measures, including cyber operations against Russian interests. In late October 2016, the Ukrainian hacking group Cyber Hunta published online emails and documents related to Vladislav Surkov, a close advisor to the Russian president. These leaks provided proof of Russian involvement in the separatist movements in eastern Ukraine.[15] Some commentators consider this hack to be US-sponsored and to constitute a response; if this was to be proved, it could be considered a form of countermeasure.

13 International Court of Justice, "Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America"), (Merits), *ICJ Reports*, no. 14, 1986, p. 119,para 228.

14 United States Department of Homeland Security and Federal Bureau of Investigation, "Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security", 2016, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

15 Andrew E Kramer, "Ukrainian Hackers Release Emails Tying Top Russian Official to Uprising", *New York Times*, October 27, 2016, https://www.nytimes.com/2016/10/28/world/europe/ukraine-russia-emails.html.; François Delerue, "The Right to Respond? States and the Cyber Arena", *Turkish Policy Quarterly*, December 2017.

CONCLUSIONS

The question of the legality of sanctions under international law can be rephrased as 'who guards the guardians?', to borrow the wording from the title of this *Chaillot Paper*. A situation whereby every state can accuse another state and act unilaterally without consequences would simply result in anarchy. This is where international law comes into play. As this chapter has demonstrated, in certain circumstances measures of retorsion and countermeasures are the only tools available to states that find themselves victims of an attack – short of an armed conflict in self-defence. The EU's cyber sanctions regime falls within this category of responses.

A situation whereby every state can accuse another state and act unilaterally without consequences would simply result in anarchy.

Whereas countermeasures may constitute the most appropriate framework for states to respond to cyber operations, in practice, governments are reluctant to go down that path, at least publicly. Looking at the approaches adopted to date, it seems that states may choose to adopt a twofold response to cyber operations. On the one hand, they may adopt a public response taking the form of sanctions and other measures of retorsion. This public response would target both the wrongdoing state and the attention of the international community, aiming at naming and shaming the wrongdoing state and showing the readiness of the adopting state to sanction cyber operations directed against it. On the other hand, they may resort to countermeasures such as a covert response, aimed only at the wrongdoing state and at showing both the readiness and the capacity of the adopting state to act and escalate if necessary. The objective would be to deter the wrongdoing state from continuing its malicious cyber activities against the adopting state.

It is important to highlight that in addition to the unilateral measures described in this monograph – i.e. measures of retorsion, countermeasures and self-defence – the measures adopted by a state or an international organisation such as the EU may be justified by a decision of the UN Security Council. Indeed, the Security Council might designate a specific cyber operation as a 'threat to the peace, breach of the peace, or act of aggression' (Article 39 of the Charter of the United Nations) and can thus make recommendations (Article 40) or take measures that can involve armed force (Articles 41 and 42). The UN Security Council may thus decide on certain actions against a state responsible for a cyber operation that will be implemented by the UN member states and other international organisations. The UN has already developed and applied criteria for designating individuals who have provided cyber support (such as web-hosting) for the commission of acts of terrorism.

CHAPTER 5

COSMIC DUST

Attribution and evidentiary standards

INTRODUCTION

Among the primary conditions to ensure the effectiveness of cyber sanctions is the capacity to link an individual or entity to a specific cyberattack, as well as clarity regarding the evidentiary standards. This is generally referred to as the challenge of attribution. With the member states retaining the primary responsibility for decisions about attribution, the role of the EU institutions in this domain and the question of shared situational awareness and political judgment will play a key role in how the EU cyber sanctions regime is implemented.

Constellation of issues in this chapter

Formally distinct from the concept of listing (i.e. the formal legal process of placing an individual or an entity on a sanctions list), attribution has become a central element in the discussion about consequences and ending impunity in cyberspace. In the same way that cosmic dust used to annoy astronomers as it obscured objects they wished to observe, the question of attribution is sometimes dismissed as receiving too much attention in the discussion about imposing consequences on malicious actors in cyberspace. Different policy communities have taken different approaches to how central attribution and evidentiary standards are for an effective cyber sanctions regime, ranging from the dismissive ('Do you need to see Putin on your keyboard?') to the conservative ('How do you want to win the court case?'). Therefore, while some consider it solely a hindrance that complicates the process of imposing consequences and ensuring adherence to international law and norms of responsible state behaviour, others see it as a significant and vital component that can reveal basic information about the tension between politics, justice and the rule of law in cyberspace.

Attribution has become a central element in the discussion about consequences and ending impunity in cyberspace.

The purpose of this chapter is to explain some of the main dilemmas linked to the challenge of attribution, in particular regarding the attribution of responsibility for cyberattacks to states. Even though currently the EU's sanctions regime does not target states but only individuals and entities, it is generally acknowledged that most of the attacks with significant effect require some level of support from a state. That

also implies that even though formally it will be individuals and entities who end up on the sanctions list, it might be politically difficult (if not impossible) to distinguish between the nationality or location of an individual and a potential state sponsor. Even though it is possible that the EU's sanctions regime might target 'lone cyber wolves' – individual hackers acting without any guidance or with no connection to a state – the experience to date shows that in most known cases there is a link between a perpetrator and a state. Therefore, the following sections discuss the challenges of attribution and state responsibility primarily through the prism of international law.[1]

SHADES OF ATTRIBUTION

Imposing a sanction equals assigning responsibility for a cyber activity or for failing to prevent such an activity from occurring. Attribution refers to the process of assigning the responsibility for an act or conduct to a perpetrator. Attribution is the first question that needs to be answered in order to establish the right course of action dictated by international law (in the case of state responsibility) or domestic laws (in the case of individuals and entities). However, capacity to attribute responsibility for a malicious cyber incident is a precondition for an effective response. One of the existing challenges in the implementation of a sanctions regime, as mentioned in previous chapters, is the difficulty in clearly establishing links between states and the perpetrators of cyber operations: state proxies (i.e. individuals and state agents whose conduct is attributable to states) or other subjects of international law. For this reason the Council Decision and Regulation provide a broad set of criteria for listing an individual or entity. But Council Decision 2019/797 also makes it abundantly clear that targeted sanctions should be differentiated from the attribution of responsibility for cyberattacks to a third state and that 'the application of targeted sanctions does not amount to such attribution, which is a sovereign political decision taken by individual states on a case-by-case basis'.

Capacity to attribute responsibility for a malicious cyber incident is a precondition for an effective response.

Attributing a cyber operation implies three different dimensions: identification of the computers and networks that were used for the launch and conduct of the operation; linking the operation to its human perpetrators; and the potential imputation of a wrongdoing to a state, if the perpetrator acted on behalf of that state. Each of these three dimensions is distinct and independent, and it is sometimes possible to identify the responsible state even without any knowledge of the computer used to carry out the attack or the individuals involved. This would be the case, for instance, when a state is able to attribute the cyber operation because its intelligence services intercepted communications on the perpetration of the cyber operation from the responsible state.

In recent years we have seen an increasing number of cases of public attribution whereby individual states have decided to point a finger in a specific direction. This has been, for instance, the case of North Korea and Russia whose links to the WannaCry and NotPetya attacks respectively have been documented and presented to the public. However, it is important to dissociate public attribution from the other dimensions of attribution. Public attribution refers to the decision to publicly name a state or another actor believed to be behind a specific cyber activity. Even when attribution is possible, a state may prefer not to publicly attribute the

1 For the discussion of other dimensions of attribution in cyberspace, see for instance: Sven Herpig and Thomas Reinhold, "Spotting the Bear: Credible Attribution and Russian Operations in Cyberspace", in Nicu Popescu and Stanislav Secrieru (eds.), "Hacks, Leaks and Disruptions: Russian Cyber Strategies", *EUISS Chaillot Paper* no 148, October 2018.

cyber operation due to other considerations, such as the geopolitical context and the need for confidentiality with regard to intelligence sources and techniques. As well as being political, the process of public attribution has legal, forensic and technical dimensions. Attribution to a machine from which the cyber operation was prepared, launched or transited, or a person, is mainly based on technical and forensic methods, while attribution to a state is mainly a political decision based to some extent on international law and factual evidence. It is clear that international law cannot resolve the technical problem of attribution.

ATTRIBUTION IN THE LAW OF STATE RESPONSIBILITY

The state is an abstract entity but it is not a black box. States operate through their agents: individuals or entities acting under the authority of a state to which actions are attributed. States may also operate through individuals and entities who are not in a hierarchical relationship to the organs of the state or who are linked informally to state institutions. The attribution of conduct to a state is an important question in international law.

It is clear that international law cannot resolve the technical problem of attribution.

In the context of the law of state responsibility,[2] the state bears responsibility for an act if three criteria are fulfilled: (i) the act is attributed to the state; (ii) the conduct constitutes an internationally wrongful act; and (iii) there are no circumstances precluding wrongfulness of the act. Alternatively, in some cases, even if a cyber operation is not attributed to a state, that state may be still held responsible according to the principle of due diligence. It is the question of establishing the link between the state and the wrongful act that is key for the discussion about potential sanctions. It is undisputed that the rules on state responsibility governing attribution apply to cyber conduct insofar as international law applies to states' activities in cyberspace. Cyber operations conducted by state organs, entities empowered to exercise elements of governmental authority or organs placed at the disposal of a state are attributable to the state, even when they are *ultra vires*.[3]

However, private individuals, acting alone or in groups, are increasingly involved in state activities. In line with the jurisprudence of the ICJ and the Articles on State Responsibility, the fact that the acts are conducted from the territory of a state[4] or conducted by citizens of a state is not sufficient reason to attribute these acts to that state.[5] In certain circumstances, however, the conduct of individuals is attributable to the state, notably if they act under the instructions, direction or control of the state, if they use public power in the absence or default of the state, and finally if the state endorses *a posteriori* their conduct.[6] While operations conducted by the military, intelligence or cybersecurity agencies of a state would meet the criterion of state responsibility insomuch as

2 See generally: François Delerue, "International Law in Cyberspace Matters : This Is How and Why", *Ideas in Focus*, EU Cyber Direct, May 16, 2019, https://eucyberdirect.eu/content_research/international-law-in-cyberspace-matters-this-is-how-and-why/

3 Articles on Responsibility of States for Internationally Wrongful Acts (adopted by the International Law Commission at its fifty-third session in 2001, annexed to General Assembly resolution 56/83 of 12 December 2001, and corrected by document A/56/49(Vol I)/Corr4), Articles 4-7.

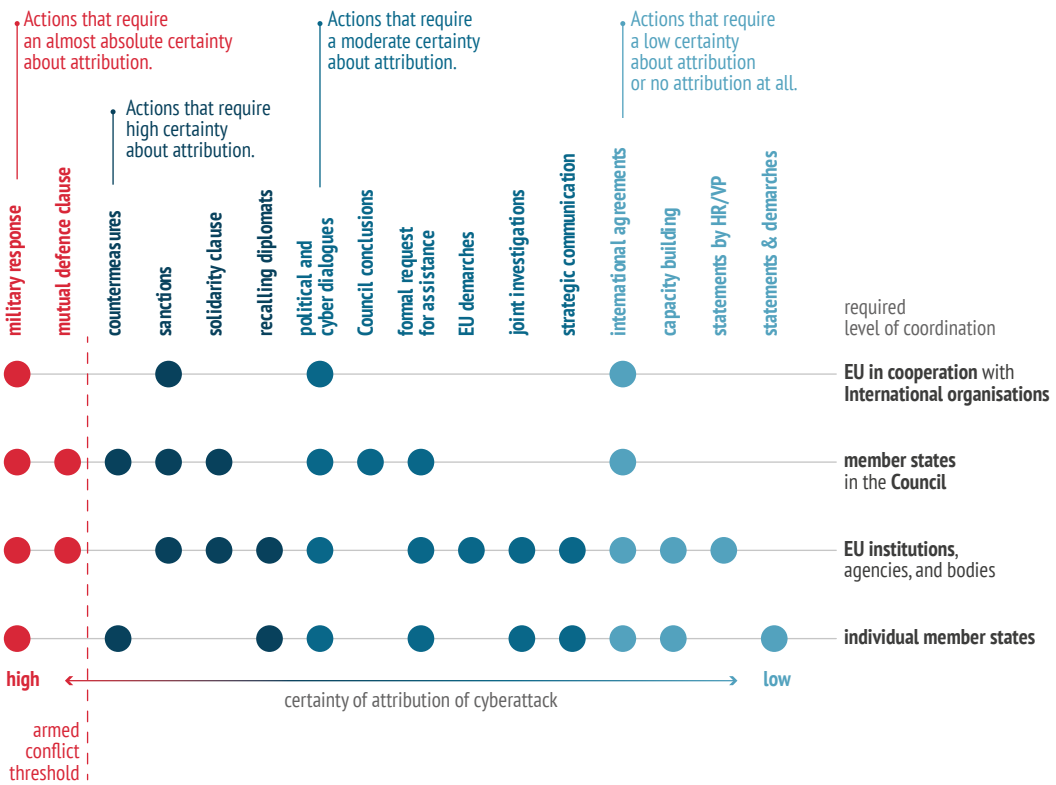
4 International Court of Justice (ICJ), *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v Albania)* (Judgment on the Merits) *ICJ Reports*, 1949, para. 4-18.

5 Olivier De Frouville, "Attribution of Conduct to the State: Private Individuals", in Alain Pellet *et al* (eds), *The Law of International Responsibility* (Oxford: Oxford University Press, 2010), pp. 261–64.

6 Articles on Responsibility of States, *op. cit.*, Articles 8-11.

Cyber diplomacy tools

and the certainty of attribution



Disclaimer: The categories proposed in this figure are a simplification. In reality, each action needs to be taken on a case-by-case basis and be preceded by a detailed legal analysis.

Data: EUISS, 2017

they are its organs, such operations conducted by a company owned by a state might be considered insufficient grounds for attribution. Similarly, a state would carry responsibility for actions of a non-state actor engaged in disruptive operations targeting financial or election infrastructure under that state's directions.

In some cases, the degree of control required for the attribution of an act perpetrated by a non-state actor under the instructions, direction or control of the state might amount to an excessively high threshold to be applicable and relevant to the use of new technology. At the same time, we should also be wary of lowering the threshold too significantly. Reflection is thus needed in order to define the most appropriate threshold to cater for attribution in cases of cyber operations. There are two main reasons underlying this situation: the internet offers the easiest way to coordinate activity without the need for any formal structures and cyber operations offer an easy means to act and to incentivise others to act. For instance, 'arming and training' means the physical delivery of weapons and the sending of agents to train the individuals on how to use these weapons. In cyberspace, the same objective can be achieved with more ease: but establishing the responsibility of, for instance, a state delivering a vulnerability to a non-state actor with the intent to perform a cyberattack may not be that straightforward.

STATE PRACTICE ON ATTRIBUTION

Over the last decade, a growing number of states have publicly attributed cyber operations to other states. Attribution is the sovereign decision of each state and therefore most of them are made through unilateral declarations. However, cases of joint or collective attribution have increased over time. Several states have almost simultaneously attributed WannaCry and NotPetya to North Korea and Russia respectively. On 4 October 2018, the UK and the Netherlands presented the first joint attribution relative to cyber operations, via a statement by the British Prime Minister, Theresa May, and the Dutch Prime Minister, Mark Rutte, attributing several operations to the Russian military intelligence agency, the GRU. These included attempts to undermine the international sporting institution, the World Anti-Doping Agency (WADA), disrupt transport systems in Ukraine, and destabilise democracies and target businesses. The same day, the two states released separate statements detailing the content of their respective attributions. Simultaneously to this joint attribution, four other states – Australia, Canada, New Zealand and the US – took part in a related collective attribution of actions to the Russian Federation. Concerning the US, it charged seven presumed agents of the GRU with cyber and disinformation operations the same day. In addition, states and international organisations – including France, the EU and NATO – made supportive statements without attributing any operations specifically to the GRU. The Russian Federation has rejected the accusations and arguments describing them as 'strong paranoia', an 'anti-Russian spy mania campaign accompanied by deliberate leaks in the media', or 'staged propaganda campaigns.' Attempts at collective attribution by NATO allies have also been ridiculed as enacted 'at the command of Washington.' Specifically, Russia maintains that public attribution is used as a tool to create 'an additional pretext for sanctions or other measures to pressurise Russia.' [7]

Such declarations – beyond the 'naming and shaming' effect – do not always lead to concrete responses. Firstly, the attributing state may have limited options to act against these states. The attributing states had previously placed serious constraints on North Korea and Iran through country-specific sanctions, and, as highlighted by Thomas P. Bossert, the then Homeland Security Advisor to US President Donald Trump, in his speech attributing WannaCry to North Korea, they may be short of options: 'President Trump has used just about every lever you can use, short of starving the people of North Korea to death, to change their behaviour. And so we don't have a lot of room left here to apply pressure to change their behaviour.'[8] Secondly, the harm caused by cyber operations is not always significant and can be qualified as a mere breach of territorial sovereignty which allows for a limited number of lawful unilateral measures that can be adopted by a victim state.

FROM COLLECTIVE ATTRIBUTION TO COLLECTIVE RESPONSE

The development of joint and collective attribution is also relevant from the point of view of its implications for the development of collective responses. The EU's framework for a joint diplomatic response to malicious cyber activities, the EU Cyber Diplomacy Toolbox, is an

7 "Russia slams 'hypocrisy' of new Western sanctions ahead of Crimea anniversary", *Euractiv*, March 18, 2019, https://www.euractiv.com/section/europe-s-east/news/russia-slams-hypocrisy-of-new-western-sanctions-ahead-of-crimea-anniversary/

8 Thomas P. Bossert, "Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea", The White House, December 19, 2017, <https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/>.

example of such an initiative. However, some of the joint response mechanisms – and the sanctions regime in particular – rely heavily on the capacity to establish a link between an attack and a perpetrator. Given that attribution remains a sovereign right of each member state and that each country works with its own intelligence and analysis – in addition to the assessments and analysis provided by EU bodies such as CERT-EU and INTCEN – arriving at a collective understanding might be difficult. The EU member states have very diverse approaches towards (public) attribution of cyber operations, which may complicate the future implementation of this framework. France still refrains from attributing cyber operations publicly, while others, notably the UK and the Netherlands, have decided to take part in joint attribution with non-EU states.

While collective self-defence is permitted under international law, collective countermeasures are not.

With regard to a potential collective response, it is important to note that while collective self-defence is permitted under international law, collective countermeasures are not.[9] Here it is important to recall the difference between measures of retorsion (such as targeted sanctions against individuals and companies, expulsion of diplomats) and countermeasures (such as sectoral and country-specific sanctions). This has important consequences in the cyber realm: since most cyber operations remain below the threshold of an armed attack, only countermeasures may be adopted in response. In such cases, the victim state would have to respond by itself only, and not collectively. It may, however, benefit from the aid and assistance of third states, without the third state conducting countermeasures itself.[10] It must be clarified, however, that this legal limitation should not be interpreted as limiting the possibility to coordinate the sanctions through alliances or a common framework such as the EU Cyber Toolbox. International law prohibits a non-victim state from justifying unlawful acts it may impose as a countermeasure conducted on behalf of the victim state.[11] Conversely, this is without consequence for the right of non-victim states to adopt measures of retorsion, in which category fall most sanctions that may be adopted, as well as to take part in a collective attribution.

THE JUDICIALISATION OF ATTRIBUTION

The attribution of a conduct by a state to another state usually takes the form of a statement by the former. Yet, in the context of cyber operations, another practice has emerged, notably in the United States, consisting of charging identified state agents with having carried out a cyber operation, and thus indirectly attributing the activity to a state. This 'judicialised attribution' may be conducted alone or in conjunction with other forms of attribution. For instance, on 6 September 2018 the US Department of Justice announced formal charges against Park Jin Hyok, a North Korean citizen, for his involvement in malicious cyber activities including the Sony Pictures hack, Central Bank cybertheft in

9 See: Pierre-Emmanuel Dupont, "Countermeasures and Collective Security: The Case of the EU Sanctions Against Iran", *Journal of Conflict & Security Law*, vol. 17, no. 3 (2012): pp. 301-36.

10 It should be noted, however, that some states and scholars advocate the existence of a right of collective countermeasures pursuant the law of state responsibility. See, for instance: President of Estonia, "President of the Republic at the Opening of CyCon 2019", May 2019, https://president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/

11 It is important to note at this stage, however, that the thematic sanctions adopted by the UN as part of its sanctions regime or under the EU's autonomous sanction regimes target specific violations of international law or are adopted in response to persistent violations of international law such as the human rights conventions or the UN Security Council resolutions. Sanctions in such cases are political instruments tantamount to countermeasures that do not require any specific evidence to be presented.

Bangladesh, and WannaCry.[12] The complaint alleges that he was a member of a government-sponsored hacking team known as the 'Lazarus Group', and worked for the North Korean government front company, Chosun Expo Joint Venture, to support the DPRK government's malicious cyber actions.[13] The same day, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) announced new sanctions against 'one entity and one individual tied to the Government of North Korea's malign cyber activities,' the concerned entity and individual being respectively Chosun Expo Joint Venture and Park Jin Hyok.[14] Park Jin Hyok is believed to be in North Korea and the FBI has issued a search warrant for him.[15] Yet, there is little chance that Park Jin Hyok will travel to the United States or to any country which would extradite him to the United States. This makes it highly unlikely that he will ever face justice. For the same reasons, the sanctions adopted against him by the Department of the Treasury have a limited effect since most of his assets are located in North Korea. The US has charged *in absentia* other state agents in the cases of cyber operations allegedly conducted on behalf of China, Iran, North Korea and also Russia.

The US's approach is interesting for the EU in as much as it already has a well-established law enforcement cooperation mechanism (through Europol or Red Notice alerts issued by Interpol) while still developing the operational dimension of the sanctions regime. The main challenges in that respect are linked to timespan and due process considerations that drive political and legal approaches to sanctions. While sanctions as a political tool can be adopted instantly if there is sufficient political will to do so, the law enforcement cases are usually built over years in order to ensure that they stand in the court of law. While in the criminal law context, the indictment expresses the government's conviction that the collected evidence *may* lead to a successful conviction in the court, the political decision to publicly attribute an attack to an individual or entity expresses definite conviction as to the guilt and leaves it to the court of public opinion to decide whether the political assignment of guilt is justified. Consequently, it could be argued that resorting to criminal indictments – which usually come with a lengthy explanation of the background to the decision, including a clear statement of the domestic law that has been violated and criminal sanctions associated with it – offers a more transparent and less politicised approach.

Charging alleged state agents is an effective tool for conveying a message towards the responsible state, without directly naming and shaming it.

In cases of public attribution to individuals or organs of a state that have been made to date, on the other hand, we have not seen a similar level of detail, primarily due to the fact that there is no such requirement under international law. In addition, approaching the problem of attribution from the international law perspective does not always provide clarity on which norms or provisions of international law have been violated. At the same time, the judicialisation of attribution also bolsters the sanctions policy of the state. The sanctions are not adopted against a state allegedly responsible for a cyber operation, but against the individuals and entities that have been identified by the authorities as perpetrators of malicious cyber activities and who benefit from the protection of another state (usually the one

12 United States Department of Justice, "United States of America v. Park Jin Hyok" (Criminal Complaint before the US District Court for the Central District of California, case MJ18-1479 2018), https://www.justice.gov/opa/press-release/file/1092091/download.

13 United States Department of Justice, "North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions" (US Department of Justice, Press release 18-1452 2018), September 6, 2018, https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

14 United States Department of the Treasury, "Treasury Targets North Korea for Multiple Cyber-Attacks," 2018, https://home.treasury.gov/news/press-releases/sm473>.

15 Federal Bureau of investigation (FBI), "Most Wanted – Park Jin Hyok," https://www.fbi.gov/wanted/cyber/park-jin-hyok.

linked through the attribution and where those nationals reside). In sum, charging alleged state agents is an effective tool for conveying a message towards the responsible state, without directly naming and shaming it.

EVIDENTIARY STANDARDS

The above discussion brings to the fore the question of different approaches to evidentiary standards. State practice on the public attribution of cyber operations to a state has been mainly unilateral. Interestingly, in the early cases of attribution by one state to another, very little evidence substantiating such claims has seen daylight. This is because most of the information on which such decisions are based is considered to be crucial for national security. However, there is a growing demand from the international community that an attribution be accompanied with supportive evidence. This evolution is reflected in the 2015 UNGGE Report[16] and endorsed in the UN General Assembly as one of the 'rules, norms and principles' governing this domain.[17] The proposed norm goes beyond recalling the states' obligations regarding internationally wrongful acts attributable to them under international law. It also recalls that 'accusations of organising and implementing wrongful acts brought against States should be substantiated,' meaning that states should consider all relevant information, a broader context, challenges of attribution and the nature and extent of the consequences.[18] The same section places strong emphasis on the fact that 'the indication that an ICT activity was launched or otherwise originates from the territory or objects of the ICT infrastructure of a state may be insufficient in itself to attribute the activity to that state.' The actual practice of some states exemplifies this development: whereas the United States' attribution of the Sony Picture hack to North Korea in 2014 was not accompanied by supporting evidence, the attribution to Russia of the 2016 DNC hack was substantiated by the release of a supportive report.[19]

In most cases, the decisions about attribution involve gathering of all-source intelligence which states are unwilling to disclose.

With regard to evidence itself, there are three main challenges that need to be addressed in the context of attribution. First, in most cases, the necessary information and evidence required to identify the computers and individuals involved, as well as any sponsoring state, might be located in a foreign country. The identification and attribution processes may depend on the goodwill and cooperation of the foreign state. In that perspective, the Budapest Convention on cybercrime adopted in 2001 contains useful principles on international cooperation and mutual assistance (Articles 23 and 24 respectively). In June 2017, negotiations started for the adoption of a second additional protocol to the Budapest Convention that focuses on international cooperation and electronic evidence. Such a protocol would notably contribute to facilitate cross-border access to electronic evidence for criminal investigations.

Second, even though specialised government agencies and digital forensics companies have

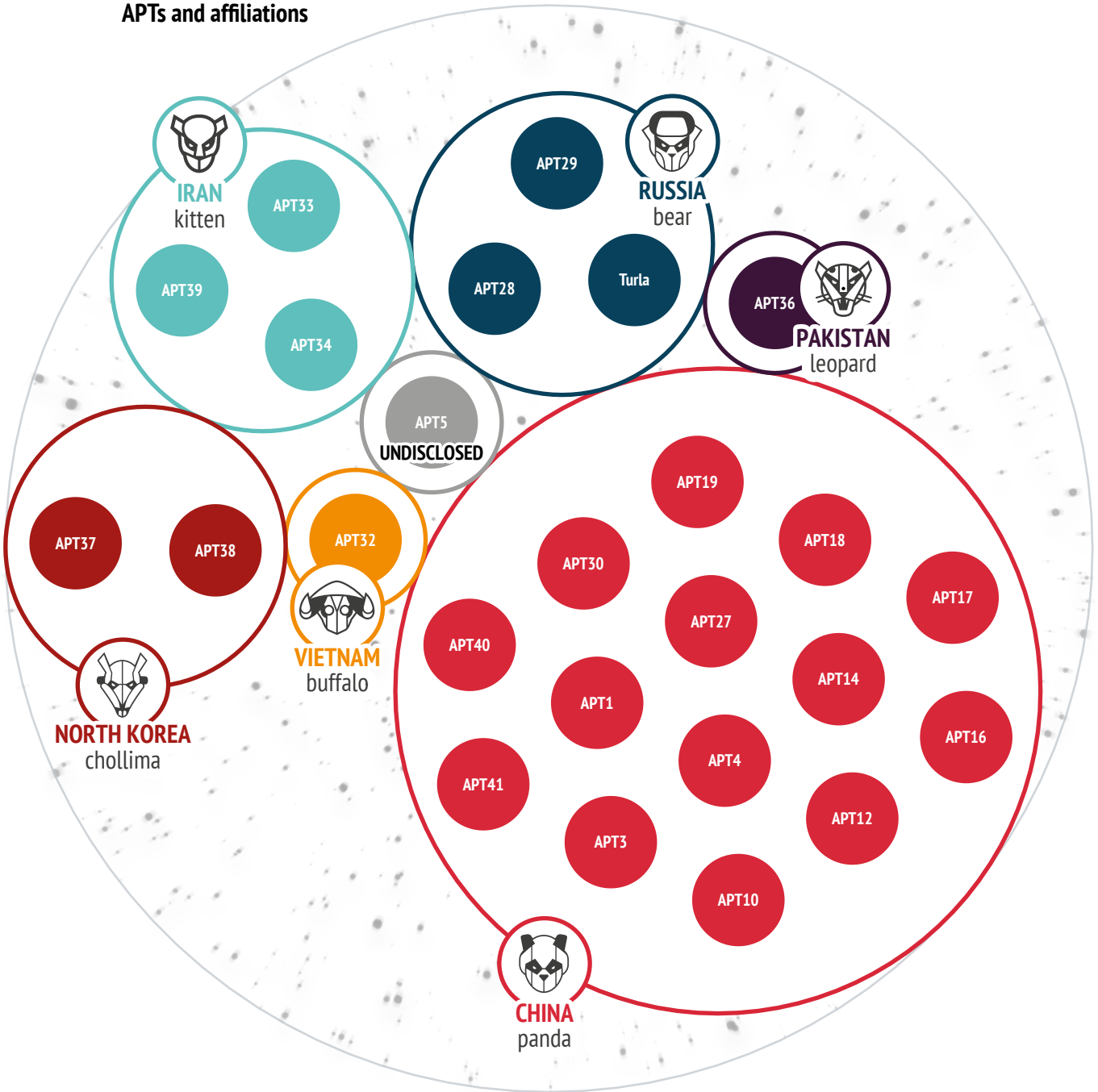
16 United Nations General Assembly (UNGA), "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," UN Doc A/70/174, para 28(f). July 22, 2015.

17 United Nations General Assembly (UNGA), "Developments in the field of information and telecommunications in the context of international security", UNGA Res 73/27 (December 11, 2018) UN Doc A/RES/73/27; "Advancing responsible State behaviour in cyberspace in the context of international security", UNGA Res 73/266 (January 2, 2019) UN Doc A/RES/73/266.

18 UN Doc A/RES/73/27, para 1.2.

19 United States Department of Homeland Security and Federal Bureau of Investigation, "Joint Analysis Report: GRIZZLY STEPPE – Russian Malicious Cyber Activity", 2016, https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf>.

APTs and affiliations



Data: FireEye, 2019; Crowdstrike, 2019

well-established operating procedures in place to collect and handle evidence, there are numerous reasons why states are reluctant to disclose such information to a broader public or even use it in court proceedings. For instance, the collected evidence and intelligence might contain information that would reveal capabilities, techniques and methods that a state in question possesses. By publicly disclosing information about a cyber operation, a state takes

the risk that other malicious actors might feel emboldened to reuse or exploit similar vulnerabilities to perpetrate further cyber operations. This has been demonstrated by the WannaCry ransomware attack and the wave of cyberattacks that affected a large number of people, institutions and businesses in 2017. The same year, a different group used a similar but more aggressive version of this malware, NotPetya, to attack numerous government agencies around the world.

Finally, while the production of the technical evidence regarding cyber operations takes a very specific and concrete form (malware computer code, IP addresses, logs, repeated patterns of activity, etc.), it is not sufficient to make definite claims about attribution. This is partly why such technical evidence can be falsified through so-called 'false flag' operations. In addition, the mere location of the computer established on the basis of its IP address cannot be treated as sufficient evidence given the ease with which such addresses can be changed. In most cases, therefore, the decisions about attribution involve gathering of all-source intelligence which states are unwilling to disclose.

The earlier sections of this *Chaillot Paper* have already addressed the question of the listing criteria as established by the EU's cyber sanctions regime. It is important to stress at this point that the decision about what constitutes a sufficient evidentiary base for listings will be decided by the Court of Justice of the European Union. As the experience of the previously adopted horizontal regime for terrorism has shown in the *Kadi* cases, the Court has quite significant powers in that respect. The member states' decision to pool their sovereignty – also when it comes to the judicial review of EU law and state practice – makes the EU sanctions regime different from that adopted by the United States or from those likely to be adopted by other countries in the future. While decisions to attribute and impose sanctions are political decisions that do not always require public justification, EU law and the statute of the Court of Justice impose on member states specific requirements and a high level of scrutiny concerning due process and evidentiary standards, to which other states are not subjected.

CONCLUSIONS

The issue of attribution has dominated the conversation about the imposition of meaningful consequences in cyberspace. While some of the measures foreseen in the Cyber Diplomacy Toolbox do not require assigning responsibility for a malicious cyber activity, cyber sanctions are at the other end of the spectrum. Whereas attribution is an important element in the international law of state responsibility – in that it makes it possible to assess what constitutes a legally acceptable response – the truth is that the decisions to attribute are primarily political in nature and therefore legal and political considerations cannot be neatly separated.

But the debate about attribution is often approached from the wrong angle: rather than being viewed as a means to an end, it is frequently portrayed as an end in itself. It is important, however, to establish the purpose of attribution as from the very beginning such decisions dictate what is considered as sufficient evidence. If the aim is to 'name and shame' the perpetrator, there is very little guidance on how much is enough – except for the judgment in the court of public opinion. The situation is quite the reverse if the ultimate objective is to bring the perpetrators to justice or constrain their operations through sanctions. In both these instances the evidentiary standards are likely to be higher.

Finally, attribution brings to the fore several elements that usually determine the success or failure of a sanctions regime. For instance, states need to take a decision whether to attribute certain attacks while considering the broader political implications of such decisions. This means that in some cases it might prove to be more prudent not to point a finger at the perpetrator (e.g. in order not to interfere with the ongoing criminal law investigations). At the same time, some of the dilemmas mentioned earlier are closely linked to the questions of capabilities, resources and information-sharing mechanisms. As this chapter has demonstrated, not all countries have the capacity and resources to decide about attributing attacks, opting instead to work closely with other partners or through regional organisations.

CHAPTER 6

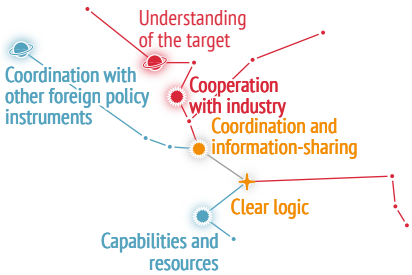
LAWS OF GRAVITATION

Due diligence obligations in cyberspace

INTRODUCTION[1]

We have established that to enhance the effectiveness of the EU sanctions regime it is necessary to ensure the sanctions' compliance with international law and communicate the underlying rationale. The high evidentiary standards established by the Court of Justice of the European Union in other types of regime (e.g. terrorist sanctions) suggests that a similar approach will be adopted in the case of the cyber sanctions regime. Does this mean that absolute certainty regarding attribution is the only way forward? This chapter introduces another concept of international law – the principle of due diligence – and demonstrates how it might become a powerful tool in making the EU's case for cyber sanctions even stronger. Like the gravitational force between all masses in the universe, the concept of due diligence brings to the fore the question of interdependence between different actors. The principle of due diligence also provides answers to two important questions about the 'laws of gravity' in cyberspace: (i) do the capacities and resources of a country determine the level of its responsibility for harm originating from its territory (*gravitational force*)?; and (ii) how does the level of interconnectedness between states influence their rights and obligations *vis-à-vis* each other (*gravitational attraction*)? In other words, to what extent are states responsible for cyberattacks originating from their territory?

Constellation of issues in this chapter



As a supporter of the rules-based international order, the EU views international law as an essential component of security in cyberspace.[2] Promotion of international law is indeed part of the DNA of the EU's CFSP.[3] It is therefore not surprising that the application of international

1 This work is supported by the French National Research Agency in the framework of the 'Investissements d'avenir' programme (ANR-15-IDEX-02).

2 European Council and Council of the European Union, *Declaration by the High Representative on behalf of the EU on respect for the rules-based order in cyberspace*, Press Release, April 12, 2019, https://www.consilium.europa.eu/en/press/press-releases/2019/04/12/declaration-by-the-high-representative-on-behalf-of-the-eu-on-respect-for-the-rules-based-order-in-cyberspace/

3 According for example to article 21 par. 2 (b) of the Treaty on European Union (TEU), one of the main objectives of EU foreign policy is to consolidate and support the principles of international law.

law and engaging states' responsibility in the event of a wrongful act are among the core objectives of the EU's cyber diplomacy.[4] The decision to place the principle of due diligence at the heart of the cyber toolbox has strengthened the EU's commitment to promote this cardinal principle of international law, including through sanctions, if necessary. By emphasising 'that malicious activities might constitute wrongful acts under international law' and that states 'should not knowingly allow their territory to be used for internationally wrongful acts using ICTs,'[5] the EU refers obviously to the famous judgment of the International Court of Justice (ICJ) in the *Corfu Channel case* where the Court declared 'every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States.'[6]

DEFINING DUE DILIGENCE IN CYBERSPACE

The prominent role of due diligence in the EU Cyber Diplomacy Toolbox is part of a more general trend initiated by the UNGGE. In 2013 already, the UNGGE affirmed that existing international norms and principles apply in cyberspace, especially international norms and principles that flow from sovereignty.[7] Sovereignty is associated with rights but also duties and responsibilities for states.[8] Sovereign states have the *right* to have their territorial integrity respected, but they also have the *duty* not to use or allow their territory to be used in such a way as to undermine the territorial integrity of another state. By virtue of their sovereignty, states have therefore an obligation of vigilance, of *due diligence*, with regard to activities taking place in their territory or under their control, whether physical or digital, public or private, national or foreign. And it is against this background of a general and well recognised principle[9] of international law that the 2015 UNGGE report acknowledged the central role of due diligence in cyberspace, affirming that 'states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.'[10]

Since 2015, several texts adopted at the international level have reaffirmed states' commitment toward this principle in cyberspace. Among the most recent ones, the G7's Lucca Declaration of 2017 recalls that 'States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs'.[11] The United Nations General Assembly resolution adopted by 119 States in December 2018 also reiterates this as an international rule, norm and principle.[12] All these declarations show that a very large majority of states consider the principle of due diligence as a fundamental principle of responsible behaviour in cyberspace. There is moreover a clear practice and *opinio juris* in favour of the normativity of due diligence. Many legal scholars and states (especially the EU member states) have

4 Council of the European Union, *Council Conclusions on Cyber Diplomacy*, Brussels, February 11, 2015, p. 7.

5 Council of the European Union, *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Activities*, 9916/17, Brussels, June 7, 2017, par.2, http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

6 International Court of Justice (ICJ), *Corfu Channel case*, Judgment of 4 April 1949, *ICJ Reports*, 1949, p. 22.

7 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report of 2013, *Note by the Secretary-General*, A/68/98, June 24, 2013, par. 19-20.

8 This close correlation between the rights and duties of sovereign states has been famously expressed by the Arbitral Award rendered in 1928 in the *Island of Palmas case*. According to it: "Territorial sovereignty [...] involves the exclusive right to display the activities of a State. This right has as corollary a duty: the obligation to protect within the territory the rights of other States, in particular their right to integrity and inviolability in peace and in war": Permanent Court of Arbitration, *Island of Palmas case*, USA v. The Netherlands, Arbitral Award of 4 April 1928, II RIAA, p. 839.

9 ICJ, *Corfu Channel case*, *op. cit.*, p. 22.

10 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report of 2015, *Note by the Secretary-General*, A/70/174, July 22, 2015, par. par. 13(c).

11 G7, *Declaration on Responsible States Behaviour in Cyberspace*, Lucca, April 11, 2017.

12 United Nations General Assembly (UN GA), A/Res/73/27, December 11, 2018, par.1.3.

expressly asserted its legally binding nature in cyberspace.[13]

However, several major cyber powers, including Russia, China, the US and the UK, call into question the legally binding nature of the due diligence obligations in cyberspace.[14] These questions or objections should not be overestimated. According to the ICJ, 'every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States'[15] is a 'general and well recognized principle'[16] of international law. Therefore, it is not necessary to identify a distinct reason for the application of this principle in the cyber context.[17] It is also well known that the US and the UK are among the greatest promoters of the application of pre-existing international law in cyberspace[18] and, as far as is known, they have never tried to demonstrate the existence of an exception excluding the application of obligations of due diligence in cyberspace.

Due diligence requires states to be reasonably vigilant with respect to the activities that are conducted within their territories according to their respective capacities.

Some scholars also seem to believe that due diligence suffers from normative vagueness that could incur states' responsibility every time they are not able to prevent or terminate a cyberattack.[19] In practice, this means that governments are unwilling to fully commit to the application of the principle of due diligence by making the case for being unable to control all the traffic – good and malicious – originating from their territory, which in turn would expose them to consequences. In fact, this criticism is largely due to a misunderstanding of the very nature of due diligence which is by definition an obligation of conduct and not of result and which implies several variability factors. It requires states to be reasonably vigilant with respect to the activities that are conducted within their territories according to their respective capacities. This means that states are not necessarily aware of everything that is happening within their territory and that they are not in a position to be able to prevent everything. On the other hand, it assumes that sovereign states cannot *reasonably* disregard everything that happens on their territory. The degree of vigilance expected is that 'of a good Government.'[20] As already shown elsewhere, due diligence is an objective principle that can be evaluated in light

13 According for example to the *Handbook on Cybersecurity*, France, Germany, the Netherlands, Spain and Finland have openly recognised due diligence as an international law rule. European Security and Defence College and the Federal Ministry of Defence of the Republic of Austria, *Handbook on Cybersecurity: The Common Security and Defence Policy of the European Union,* 2018, p. 31. For the position of legal scholars, see for example *Tallinn Manual 2.0* which recognised due diligence as a general principle of international law: M.N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), p. 30; See also, Karine Bannelier, "Cyber-Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber-Operations?", *Baltic Yearbook of International Law*, vol. 14, 2014, pp. 23-39.

14 *Handbook on Cybersecurity, op. cit.*, p. 31.

15 ICJ, *Corfu Channel Case*, *op. cit.,* p. 22.

16 Ibid.

17 M. N. Schmitt, "In Defense of Due Diligence in Cyberspace", *The Yale Journal Forum*, June 2015, p. 73.

18 See for example, the US position in H.H. KOH, "International Law in Cyberspace," United States Cyber Command Inter-Agency Legal Conference, Fort Meade, MD, 18 September 2012, *Harvard International Law Journal Online*, vol. 54, December 2012, https://harvardilj.org/wp-content/uploads/sites/15/2012/12/Koh-Speech-to-Publish1.pdf. See also the speech of UK Attorney General Jeremy Wright, "Cyber and International Law in the 21st Century," May 23, 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

19 See for example, M. Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press, 2014), p. 87; N. Tsagourias, "On the Virtues and Limitations of Cyber Due Diligence", *Agora 12: The Defence of General Interests in Cyberspace*, 13th Annual Conference of the European Society of International Law, *Global Public Goods, Global Commons and Fundamental Values: The Responses of International Law*, Naples, September 8, 2017; Eric Talbot Jensen and Sean Watts, "A Cyber Duty of Due Diligence : Gentle Civilizer or Crude Destabilizer?", *Texas Law Review*, vol. 95, 2017, pp. 1555-77.

20 International Law Commission (ILC), "Draft articles on Prevention of Transboundary Harm from Hazardous Activities," *2001 Yearbook of the ILC,* §17, p. 155.

of four main variability factors: knowledge, capacity, risk and harm.[21] These variability factors give the principle of due diligence all the flexibility and the plasticity necessary for it to be effective and to determine how obligations of diligence should apply in each case.

DUE DILIGENCE AND SANCTION DILEMMAS

As stated earlier in this *Chaillot Paper*, sanctions also have a normative function both to 'influence the behaviour of potential aggressors in cyberspace'[22] and 'to signal the commitment to a norm'.[23] The EU Cyber Diplomacy Toolbox itself states that restrictive measures must be seen in the broader context of EU cyber diplomacy as a means to influence the behaviour of potential aggressors in the long term. And it is well known that, according to the EU guidelines on restrictive measures, sanctions must be consistent with Article 21 of the Treaty on European Union (TEU), which sets among its main objectives support to the principles of international law.[24] From this point of view, EU restrictive measures serve also to enforce the principle of due diligence in cyberspace.

Due diligence could help to circumvent two major problems related to the legal regime applying to malicious activities in cyberspace: the problem of its qualification as a *violation* of international law and the problem of the *attribution*[25] to a state of a given malicious act. The qualification of malicious activities as a wrongful act, which means a violation of international law attributable to a state, can be extremely difficult to make.[26] Given the wide range of malicious cyber activities targeting EU member states, one of the main challenges is to identify available responses. While certain reactions to malicious activities are always allowed, even in cases where it is impossible to demonstrate that a state has violated an obligation of international law by action or omission,[27] others are only admissible in reaction to an internationally wrongful act committed by a state, namely peaceful countermeasures and acts of self-defence, as discussed in the previous chapter.[28] But while international law is well-settled concerning the classification of permissible reactions, the terminology used by the EU in its cyber toolbox is not very clear in this respect.

21 Karine Bannelier, "Between Certainty and Flexibility: Obligations of Conduct and Variability Factors in the Due Diligence Principle", *CyCon X: The 10th International Conference on Cyber Conflict*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, May 30-June 1, 2018.

22 *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Activities, op. cit.*, par. 4.

23 Alexandra Hofer, "Negotiating International Public Policy through the Adoption and Contestation of Sanctions", *Revue belge de droit international*, no. 2, 2017, p. 470.

24 According to the EU guidelines on implementation and evaluation of restrictive measures, sanctions "must be consistent with CFSP objectives as set out in Article 21 of the Treaty on European Union (TEU)": Council of the European Union, *Guidelines on Implementation and Evaluation of Restrictive Measures (Sanctions) in the Framework of the EU Common Foreign and Security Policy*, Brussels, June 15, 2012. par. 2. See also in this respect Council of the European Union, *Update of the EU Best Practices for the Effective Implementation of Restrictive Measures*, Brussels, March 24, 2015.

25 The Council Decision of 17 May 2019 "concerning restrictive measures against cyber-attacks threatening the Union or its Member States" makes clear that "Targeted restrictive measures should be differentiated from the attribution of responsibility for cyber-attacks to a third State. The application of targeted restrictive measures does not amount to such attribution, which is a sovereign political decision taken on a case-by-case basis. Every Member State is free to make its own determination with respect to the attribution of cyber-attacks to a third State" (Preamble par. 9).

26 It is true that, for the time being at least, the targeted sanctions of the EU do not target states but intend to deal with individuals and institutions. However, an evolution of the restrictive measures practice in the future cannot be ruled out, depending on the circumstances and the gravity of cyberattacks.

27 For example, this could be a mechanism for international cooperation and dispute settlement, acts of retorsion or exceptional mechanisms of self-protection (state of necessity, distress, *force majeure*).

28 See also, the G7 Lucca Declaration, *op. cit*: "We note that, in the interest of conflict prevention and peaceful settlement of disputes, international law also provides a framework for States' responses to wrongful acts that do not amount to an armed attack - these may include malicious cyber activities. Among other lawful responses, a State that is the victim of an internationally wrongful act may, in certain circumstances, resort to proportionate countermeasures, including measures conducted via ICTs, against the State responsible for the wrongful act in order to cause the responsible State to comply with its international obligations."

EXISTENCE OF AN INTERNATIONAL WRONGFUL ACT

Due diligence could help to resolve the problem of the *legal qualification of a cyberattack* especially when such a cyberattack is carried out by non-state actors. Under international law there is no specific prohibition of malicious cyber activities or even cyberattacks and there are no universally accepted definitions of these notions. However, depending on the nature and effects of a malicious activity or a cyberattack, several rules of international law may be violated, ranging from breaches of *jus contra bellum* or *jus in bello*, the violation of principles such as that of non-intervention, non-interference or the right of peoples to self-determination. The proposed regime enumerates a number of acts that fall under its scope, including attacks on critical infrastructure or critical state functions in the areas of defence, electoral systems and internal security, among others. However, determining which exact rule of international law has been violated in a specific attack might be difficult. There are, for example, uncertainties in the distinction between the principle of non-intervention and the principle of non-interference in the internal affairs of a country. In the same way it can be difficult to determine precisely when malicious activity constitutes a breach of sovereignty or whether cyber-espionage constitutes a violation of international law *per se*.[29]

By virtue of their sovereignty, states have an obligation to not knowingly allow their territory to be used for acts contrary to the rights of other states. Instead of putting the emphasis on the legal qualification of a malicious activity, this concept makes it possible to focus on *what could have been done* by a state, and on *what the state did not do in order to prevent transboundary cyber-harm.* Thus, without having to research whether or not the malicious cyber activity in question is the action of a state, and without having to research which *exact norm* has been violated (non-interference, non-intervention, etc.), one could focus on the fact that the state *knew* or *ought to have known* that a cyberattack had been launched from its territory and its infrastructure,[30] *had the means of acting* to prevent this cyberattack or to attenuate the effects thereof, but did nothing to try and prevent this. If a state is aware of (or should have been aware of) a cyberattack being initiated by non-state actors from its territory, and still does nothing to prevent and cease it, then it could be violating its duty of *due diligence*, thus allowing the injured state to adopt countermeasures, against it and/or against the private actors operating on its territory, until the responsible state adopts the necessary measures to end the cyberattack and prevent future attacks. This reasoning, however, has led to some confusion among the technical community in the past due to uncertainty about governments' responsibility for monitoring all egress traffic[31] and the necessity for them to implement technology that gives them the ability to inspect all such traffic. With increased traffic flows, growing use of encryption, and the decentralised nature

29 The *Tallinn Manual 2.0* seeks to determine under what circumstances a cyberattack could constitute a violation of the sovereignty of a State: see M.N. Schmitt (ed.), *Tallinn Manual 2.0*, *op. cit.*, analysis under "Rule 4 – Violation of sovereignty", §§ 10-14. See also Russell Buchan, *Cyber Espionage and International Law* (Oxford: Hart, 2018), p. 248. The EU regulation of 17 May 2019 "concerning restrictive measures against cyber-attacks threatening the Union or its Member States" defines cyberattacks as "actions involving any of the following: (a) access to information systems; (b) information system interference; (c) data interference; or (d) data interception". However, this definition has been adopted for the purpose of the regulation and does not constitute a universal definition of cyberattacks nor does it seek to identify to what extent these actions could constitute a violation of international law.

30 While knowledge is an essential component of the obligation of due diligence, few studies have been devoted to it. In the *Corfu Channel case*, the Court did however clearly underline that states have the obligation not to '*knowingly*' allow their territory to be used for purposes contrary to the rights of other states. In the digital space the element of knowledge can however raise certain questions and be a source of concern. However, the obligation of due diligence does not imply that states know everything that happens on their territory or under their control. As the International Court of Justice underlined in the *Corfu Channel case*, "it cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that that State necessarily knew, or ought to have known, of any unlawful act perpetrated therein, nor yet that it necessarily knew, or should have known the authors.": ICJ, *Corfu Channel case*, *op. cit.*, p. 18.

31 Egress traffic is defined as the volume and substance of traffic transmitted from the host network to an external network destination.

of the internet, in might be unrealistic to expect a government to exercise full control over or even have the capacity to monitor egress traffic. Nonetheless, states should put in place adequate incident response capabilities that enable them to take action when such traffic is reported.

THE CHALLENGE OF ATTRIBUTION

Attribution is one of the thorniest problems for incurring the responsibility of states in cyberspace. Attribution of a malicious activity as a technical, but also as a legal and political operation, is extremely complex. This operation is even more complex if we move from the classical paradigm of unilateral attribution made by the injured state to a pattern of collective attribution endorsed by several states as might become the case under the Cyber Diplomacy Toolbox or under G7 guidance.[32] From a technical perspective these difficulties are due to a multitude of factors, including the lack of sufficient technical capacity in many countries (the problem of 'forensic capacity') as well as the use of particularly sophisticated dissimulation techniques (such as 'spoofing' or the use of intermediate servers) which are used by hackers to make others believe the attack was launched by someone else.

The EU itself should set a good example, demonstrate its own commitment to due diligence, capacity and implementation and be in a position to help developing countries.

But attribution is also, and above all, a sovereign political decision which is adopted taking into account a much broader context.[33] An EU collective attribution is thus a very difficult task while member states do not automatically share the same political agenda or technical capacity. From this point of view, the invocation by the EU of a violation of due diligence obligations could help circumvent this problem and facilitate collective action. This is because establishing that a state has violated its obligations of due diligence does not necessarily entail *the attribution* of the cyberattack to this state using the conventional mechanisms of attribution. Due diligence is in fact relatively indifferent to issues such as whether the activity in question was committed by an organ of the state, an agent acting *ultra vires* or outside his/her functions, a proxy, an intermediary, a group of 'patriotic hackers', terrorists, the mafia, cybercriminals or just a business wishing to gain a competitive advantage. The only issues that matter in relation to due diligence are whether the elements constituting its violation are present, and whether, no matter who perpetrated the attack, the state knew or should have known that its infrastructure was being used to launch a cyberattack causing harm of a certain seriousness to another state. Has it failed in its obligation to take the reasonable measures at its disposal to prevent the harm? If the answer to these questions is positive, the liability of the state could be engaged no matter who perpetrated the acts and what their relation was with the hosting state. As summarised by the French National Cyber Defence Strategy, 'a state which has not fulfilled this obligation (of conduct) could thus in certain cases, incur its responsibility and be the object of countermeasures by the

32 "G7 plans strategy to protect against cyber attacks. Western nations propose sanctions and public shaming of Russia and other internet attackers", *Financial Times*, 6 April 2019.

33 It is worth noting, however, that several independent groups of researchers have launched initiatives aimed at building a network of organisations engaged in attribution activities, including ICT4Peace and Citizen Lab.

victim state, even if it is not the sponsor'.[34] Of course, this does not mean that the many difficulties relating to the origin and *modus operandi* of cyberattacks miraculously disappear. To demonstrate the existence of a violation of the obligation of diligence, technical proof is necessary, including establishing that the cyberattack emanates from the territory of the state in question (or has transited through it) and that the latter had (or should have had) knowledge of this situation, had reasonable means at its disposal to put an end to it (or at least attenuate the consequences) and did nothing in this regard.

CONCLUSIONS

The concept of due diligence is a complex one and its application in cyberspace can raise legitimate questions. But the answer to this complexity should certainly not be to try to delete due diligence from the list of states' obligations, but rather to explain better the nature, functions and parameters of this principle in cyberspace. As noted by the UK, 'those around the world whose behaviour international law seeks to constrain of course resent it, and they will seize on any excuse to say international law is outdated and irrelevant and can therefore be ignored. We must not give them that opportunity by conceding that applying international law principles to cyberspace is just too difficult'.[35]

It is therefore precisely by explaining how the principle of due diligence applies in cyberspace that the EU could, through the implementation of its Toolbox, play a decisive role for the enforcement of the principle globally. From this point of view, it could be interesting to underline that the principle of due diligence does not only refer to an obligation *to abstain,* intended to ensure peaceful coexistence between states; it can also be conceived as a *positive* obligation calling on states to gradually develop security measures to prevent the malicious use of their cyber infrastructure. The influence of the EU could be important in order to highlight the importance of such positive obligations. Indeed, the EU has without doubt an important role to play in order to promote standards and good practices in the field of cybersecurity. The adoption of the Network and Information Security (NIS) Directive, the introduction of a reference to this directive in the Cyber Diplomacy Toolbox, followed by the adoption of the EU Cybersecurity Act, are all steps advancing the notion that states should take appropriate measures to protect their critical infrastructure from ICT threats. Similarly, the General Data Protection Regulation (GDPR), which entered into force in May 2018, requires states and companies to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of data breaches. Many different means are suggested, such as certification, encryption, a process of regular testing, using approved codes of conduct, and approved certification mechanisms. This is a classic due diligence obligation which is of fundamental importance for the implementation of the GDPR and accompanied, here also, with the threat of sanctions and fines in case of failure to adopt the appropriate measures. We can expect that the practice of the EU in these fields, as well as its international promotion of due diligence, could provide useful indications about minimum standards in relation to this principle and what might be the consequences in the event that private actors or states fail to act in order to implement such standards. At the same time the EU itself should set a good example, demonstrate its own commitment to due diligence, capacity and implementation and be in a position to

34 Author's translation. The original version is the following: "En vertu du principe de l'obligation de diligence raisonnable qui est un principe du droit international coutumier, tout Etat à l'obligation de ne pas laisser sciemment utiliser son territoire aux fins d'actes contraires aux droits d'autes Etats. Un Etat qui n'aurait pas rempli cette obligation (de moyens) pourrait ainsi, dans certains cas, engager sa responsabilité et être l'objet de contre-mesures par l'Etat victime, même s'il n'est pas le commanditaire" : Premier Ministre, Secrétariat Général de la Défense et de la Sécurité Nationale, *Stratégie Nationale de la Cyberdéfense* (Paris: Economica, 2018), p. 102.

35 Attorney General Jeremy Wright, "Cyber and International Law in the 21st Century", *op. cit.*

help developing countries with capacity/resilience building in this field. The incorporation of many of these concrete solutions and practices into EU legislation creates a clear obligation on the part of the member states – one that needs to be enforced by the European Commission as the guardian of the treaties and by the Court of Justice of the European Union.

CHAPTER 7

MULTIPLE MOONS

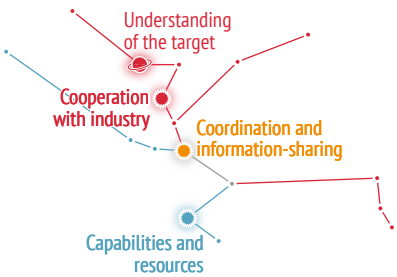
Cyber sanctions and the role of the private sector

INTRODUCTION

Cyber diplomacy is not only the business of government. It also involves numerous other stakeholders, in particular from the private sector, that circle governments like multiple moons attracted by various gravitational forces. As stated in the opening chapters of this *Chaillot Paper*, the effective use of cyber sanctioning mechanisms (e.g. travel bans and asset freezes) to coerce, constrain and/or signal behaviour in cyberspace often relies on good cooperation with industry and private actors, in particular when such technology belongs to or is operated by the private sector. The following sections discuss the different ways in which private sector actors orbit around governments and consequently play an important role in sanctions implementation, including for attribution, operational cooperation and norms development.

In addition to the potential impact of sanctions on how businesses operate (as discussed earlier on in this volume) – an aspect that has already been addressed in the literature on sanctions – it is important to highlight two alternative ways of thinking about 'cyber sanctions' as a tool used for the enforcement of norms in general. For instance, rather than targeting individuals, firms, government agencies or even sectors of economic activity in retaliation for cyberattacks, states may increasingly resort to cyber operations as a potentially less costly alternative to traditional sanctioning instruments. Some EU member states have openly admitted to conducting offensive cyber operations, such as the UK's efforts to 'take down' websites used for recruitment of terrorists or the dissemination of information about bomb-making designs. There have been instances in which the UN Security Council has taken action to designate individuals for web-hosting activities as a part of its counterterrorism efforts.

Constellation of issues in this chapter



PRIVATE SECTOR AND ATTRIBUTION

An area where private actors, in particular private cybersecurity companies, have played a critical role is in the attribution of malicious cyber activities. With access to sophisticated computer forensic capabilities, private companies offer invaluable contributions by providing relevant and timely threat intelligence to

decision-makers. Such information is usually delivered either as open source material or through more exclusive and secretive arrangements. Some of the most influential reports linking malicious cyber operations to governments and non-state actors have been released by private companies. Symantec was among the first companies to publicly disclose information about the Stuxnet malware that affected Iran's Natanz nuclear facility in 2010. In 2015, Kaspersky Lab documented the tools, techniques and procedures behind a hacking team called 'Equation Group' which is believed to be linked to the US National Security Agency (NSA). The same year, ThreatConnect, a US-based cyberintelligence firm, published the report 'Project CameraShy', in which it attributed cyber espionage activity associated with the 'Naikon' Advanced Persistent Threat (APT) group to a specific unit of the Chinese People's Liberation Army (PLA). The report demonstrated, *inter alia*, how Unit 78020 conducted cyber espionage against military, diplomatic, and economic targets in Cambodia, Indonesia, Laos, Malaysia, Myanmar, Nepal, the Philippines, Singapore, Thailand and Vietnam as well as international bodies such as the United Nations Development Programme (UNDP) and the Association of Southeast Asian Nations (ASEAN).[1] In 2018, Kaspersky research exposed a US-led counterterrorism cyber-espionage operation targeting Daesh and al-Qaeda members.[2] Such publicly available threat intelligence and forensics reports released regularly by cybersecurity companies provide useful open source evidence that might be used in the future to justify placing an individual or an entity on the EU's cyber sanctions list.

Political risks associated with a premature and potentially mistaken attribution are much higher for government agencies than for private sector companies.

That also affects the standing of these companies *vis-à-vis* state intelligence agencies which oftentimes lag behind and heavily rely on the forensic evidence provided by private cyberintelligence agencies, consequently breaking the state's monopoly on pointing fingers at potential threats.[3] There is, however, one clear difference in motivation for such extensive cooperation. Whereas state agencies are interested in knowing where the threat originates from in order to prepare adequate policy responses, for the private cybersecurity companies the primary concern is to protect their businesses and the interests of their clients, including in the member states (e.g. critical infrastructure). The potential trust issues typical for such cooperation have been partly overcome thanks to more structured and formalised partnerships with the government agencies. Through their membership in the advisory bodies, many of them have established permanent channels for engagement with the EU agencies, such as the Advisory Groups on Financial Services, Internet Security and Communication Providers with the Europol's European Cybercrime Centre (EC3) or the Advisory Group of the EU's Cybersecurity Agency (ENISA). The Industry 100 initiative by the UK's National Cyber Security Centre (NCSC) is another illustration of a more integrationist approach. Through the initiative, industry secondees work across a wide range of short-term placements at the NCSC, usually on a part-time basis.

In recent years, the private sector has been active in attributing malicious cyber operations to non-state actors associated with Russia, Iran, China, North Korea and the United States. While this has proven to be a growing business,

1 ThreatConnect and Defense Group Inc, *Project Camerashy. Closing the Aperture on China's Unit 78020* (Arlington, VA: ThreatConnect, 2015).

2 Chris Bing and Patrick Howell O'Neill, "Kaspersky's 'Slingshot' report burned an ISIS-focused intelligence operation", *Cyberscoop*, March 20, 2018.

3 Sasha Romanosky, "Private-Sector Attribution of Cyber Attacks: A Growing Concern for the U.S. Government?", *Lawfare*, December 21, 2017.

many companies also point out that technical evidence provides insufficient grounds for political attribution and refrain from this type of activity. Furthermore, cybersecurity companies point out the fact that the growing accessibility and impact of cyber operations means that an increasing number of countries may embrace newly-available tools and techniques in the future. Such a politically powerful instrument needs to be handled with care. Political risks associated with a premature and potentially mistaken attribution are much higher for government agencies than for private sector companies. Therefore, governments need to be cautious and maintain a certain distance from such reports in order to avoid potential destabilisation and conflict with third countries. At the same time, some countries have expressed scepticism towards such reports due to the fear that given the location of tech companies in the US or Europe, some of them might deliberately do the governments' bidding.

To mitigate such risks, different initiatives have been launched to investigate the feasibility of establishing an international consortium that could enforce a standardised framework for threat actor-naming conventions and bring more transparency into reporting mechanisms, including indicators of compromise (IoCs).[4] There is also an initiative underway among university-based centres and laboratories located in different countries, for a neutral, third-party attribution network that could combine technical knowledge of cyberattacks with political and institutional analysis of the motivations of potential attackers.

PRIVATE SECTOR AND NORM ENTREPRENEURSHIP

In addition to state-led processes, several non-state initiatives spearheaded by the private sector have emerged as an important avenue for establishing norms of responsible behaviour in cyberspace, resulting in new relationships and dependencies for private-public relations.[5] While seemingly insignificant, such initiatives might in the longer term establish the foundations of a new normative framework for state behaviour in cyberspace – one that might also rely on sanctions for its enforcement.

There are many reasons why private companies, whose primary focus is on profit and rewarding stakeholders, might be involved in such undertakings. Most see it as a way of creating a more favourable environment for conducting their business. Businesses thrive in stable regulatory environments, and the use of cyberspace for interstate conflict could undermine the overall trust in the digital environment and consequently affect the operations of companies. Similarly, the limited trust between governments and uncertainty about their intentions towards one another might have a negative impact on businesses by making their operations more difficult and costly.

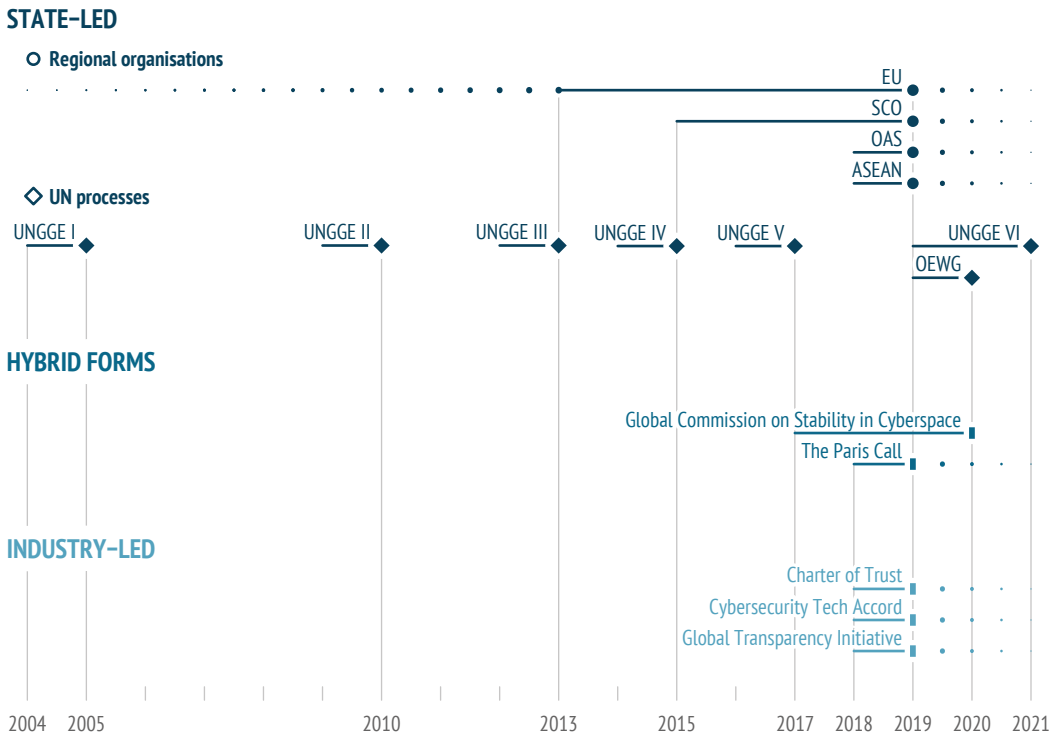
Private sector-led initiatives such as the Cybersecurity Tech Accord, the Charter of Trust, or the Global Transparency Initiative (spearheaded by Microsoft, Siemens, and Kaspersky respectively), have been regarded by governments as valuable self-regulatory initiatives, albeit resulting in little change in how states behave in cyberspace. The Tech Accord promotes a safer online environment 'by fostering collaboration among global technology companies committed to protecting their customers

4 For instance, the 2017 report by RAND recommends establishing a Global Cyber Attribution Consortium. See: John S. Davis II *et al.*, *Stateless Attribution. Toward International Accountability in Cyberspace*, RAND Corporation, 2017.

5 Jacqueline Eggenschwiller, "International Cybersecurity Norm Development: The Roles of States Post-2017", *Research in Focus*, EU Cyber Direct, March 2019.

Norms in cyberspace

Timeline of key initiatives



Data: international orgnisations' and industry websites, 2019

and users and helping them defend against malicious threats'. This position has emerged from an increasing conviction among Microsoft leaders and other companies that states are no longer only their counterparts in policymaking or regulators working for the benefit of their societies through the use of new technologies, but are also increasingly responsible for causing damage to internet users – and their clients – around the world. In that sense, while acknowledging the responsibilities of the private sector, the Tech Accord assigns a fair amount of blame for instability in cyberspace to state actors.[6] In this new environment, private companies like Microsoft take on the traditional role reserved for governments, including the commitment to 'do more to protect and defend ... customers around the world' and calling on world leaders to 'implement international rules to protect the civilian use of the internet'.[7]

It is exactly this expansionist agenda, with private sector actors acceding to new functions traditionally reserved to governments, that has caused uneasiness among political leaders. A similar initiative, albeit more focused on self-regulation and promoting closer public-private cooperation, was launched by Siemens with the Charter of Trust. The initiative calls for binding rules and standards to build trust in cybersecurity and further advance digitalisation. To achieve these objectives it

6 This approach is clearly visible in commitments such as: 'We will not help governments launch cyberattacks against innocent citizens and enterprises from anywhere' and 'We will strive to protect all our users and customers from cyberattacks – whether an individual, organization or government – irrespective of their technical acumen, culture or location, or the motives of the attacker, whether criminal or geopolitical'.

7 Brad Smith, "The Need for a Digital Geneva Convention," *Microsoft Blog*, February 14, 2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

proposed ten principles, including ownership of cyber and IT security, responsibility throughout the digital supply chain, certification for critical infrastructure and solutions, security by default, and user-centricity.

This type of norms entrepreneurship has evolved relatively quickly towards more hybrid formats that have led the private sector to work together with governments and civil society representatives. The best illustration of this kind of multi-stakeholder normative undertaking is the Paris Call for Trust and Security in Cyberspace launched at the Internet Governance Forum in 2018. Spearheaded by Microsoft and the French government, the Paris Call has over 500 signatories and has been endorsed by the European Commission. The text of the Paris Call – the outcome of negotiations between different groups – is a mix of normative commitments based on UN-driven processes and bottom-up driven commitments. Supporters of the Paris Call have agreed, *inter alia*, to increase prevention against and resilience to malicious online activity; protect the accessibility and integrity of the internet; cooperate in order to prevent interference in electoral processes; prevent the proliferation of malicious online programmes and techniques; and clamp down on online mercenary activities and offensive action by non-state actors.

Governments rely on the private sector for forensic and strategic information, thereby turning the security companies into quasi-intelligence agencies.

Some private sector companies have also invested heavily in initiatives aiming to protect their own reputation by promoting the norm of transparency. Microsoft was among the first companies to launch the Government Security Program (GSP) – an initiative with a global scope that provides national governments with controlled access to Microsoft Windows source code and other technical information they need in order to be confident in the enhanced security features of the Windows platform. As a Russia-based company with a global presence, Kaspersky Lab has often been accused of having too close ties with the Kremlin and portrayed as presenting a 'grave threat' to US national security. As a consequence, in 2017 President Trump signed into law legislation that bans the use of Kaspersky Lab products and services in federal agencies.[8] In an unprecedented move towards regaining its reputation and international credibility, the company launched the Global Transparency Initiative aimed at engaging the broader information security community and other stakeholders in validating and verifying the trustworthiness of its products, internal processes, and business operations. It has also established three Transparency Centres in Switzerland, Spain and Malaysia that provide the opportunity to review the company's code, software updates, threat detection rules and other technical and business processes.[9] To dismiss some of the concerns about the company's use of personal data, Kaspersky also decided to relocate its data storage and user data processing facilities from some regions as well as its software development infrastructure from Moscow to Switzerland. A similar approach was adopted by the Chinese company Huawei amidst the debate linked to its 5G service. In May 2019, Huawei decided to open a Cyber Security Transparency Centre in Brussels to showcase Huawei's end-to-end cybersecurity practices, to facilitate communication between Huawei and key stakeholders on cybersecurity strategies and end-to-end cyber security and privacy protection practices, as well as to provide a product security testing and verification platform. This initiative complements the Huawei Cyber Security Evaluation Centre, operating since November 2010 under a set of arrangements

8 In 2018, Kaspersky filed lawsuits challenging the ban on its products in US government systems as stipulated by a Binding Operational Directive from the Department of Homeland Security and the 2018 National Defense Authorization Act.

9 As of 3 October 2019.

between Huawei and the UK to mitigate any perceived risks arising from the involvement of Huawei in parts of the UK's critical national infrastructure.[10]

PRIVATE SECTOR AND CYBER-ENABLED SANCTIONS

Another form of active intervention is undertaken not by states and international organisations, but by major private firms, often in cooperation with law enforcement agencies or on the basis of government regulation. These are not (yet) considered traditional types of sanctions as incarnated in the sanctions regime adopted by the EU – even though they have a sanction-like effect. In such cases, companies may opt to use some of the tools and instruments at their disposal to deny or limit access to their services and products to users who violate their contractual obligations or other norms of responsible behaviour. Such actions could eventually take the form of what might be classified as cyber-enabled sanctions. Examples of such activities include Microsoft's takedown of botnets and Facebook's stepped-up efforts to block the access of users engaged in electoral interference and the proliferation of hate speech. Mentioning these instruments and understanding their functioning is important as they might in the future become as relevant as asset freezes and travel bans. This will require implementing additional legal and technological solutions but is not impossible.

Fight against cybercrime

Botnets – networks of computers infected with malware – are one of the most common methods used by cyber criminals to execute phishing and ransomware attacks (e.g. Avalanche) or to distribute spam (e.g. Srizbi, Rustock). Malware allows criminals to take control of multiple infected computers at a distance and perform attacks using one or more command and control (C&C) servers, making them capable of launching malicious attacks on a massive scale. The private sector plays a key role in helping take the botnets down, which from the technological point of view is a sanctioning mechanism (i.e. a restrictive measure imposed for a political goal or purpose). In 2015, Europol's Cybercrime Centre (EC3) led an international campaign against the Ramit botnet whose primary goal was to harvest credentials such as online banking log-ins, passwords and personal files. Microsoft's Digital Crime Unit took part in the takedown, alongside other industry partners Symantec and AnubisNetworks, by assisting Europol and national investigators from Germany, Italy, the Netherlands and the UK with shutting down the C&C servers and redirecting 300 internet domain addresses used by the botnet's operators.

There are also 'hack backs' undertaken by governments, as in the case of the government of the Netherlands intruding into the systems of cyber criminals. In one specific case, the Dutch National High Technology Crime Unit discerned the use of cryptographic software in a money laundering investigation, and identified an undisclosed issue with the service that allowed them to decrypt the criminal's communications.[11] In another widely reported case in 2018, the Dutch AIVD intelligence service gained access to systems operated by a Russian hacking group which was widely considered to be state supported,[12] and maintained this level of access

10 Cabinet Office, "Huawei cyber security evaluation centre oversight board: annual report 2019", March 28, 2019, https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019.

11 Lisa Vaas, "258,000 encrypted IronChat phone messages cracked by police", November 9, 2018, https://nakedsecurity.sophos.com/2018/11/09/258000-encrypted-ironchat-phone-messages-cracked-by-police/

12 Rick Noack, "The Dutch were a secret U.S. ally in war against Russian hackers, local media reveal", *Washington Post*, January 26, 2018.

for at least one year. The use of 'hack backs' as a self-help mechanism[13] by private companies has caused a lot of controversy, with government officials taking a clear stand against such practices as 'negatively affecting the already unclear rules of engagement in cyberspace'.[14]

Fight against terrorism

The private sector plays a relevant role also in the context of fighting terrorism. The UN's 1267 Sanctions Committee concerning Daesh, al-Qaeda, and associated individuals and groups has adopted designation criteria for individuals providing web-hosting services under the rubric of 'material support for the commitment of acts of terrorism or incitement to commit acts of terrorism.' Internet hosting or cyber support has been included in 36 statements of case (designations of individuals where internet hosting was cited) as of February 2017, but significantly, it has never been the sole criterion for a listing. There is some reluctance (typically on the part of the US, due to first amendment concerns) to make this the principal basis for a designation, something that according to some observers can lead to gaps in enforcement, limiting the capacity of the committee to act in some instances. In theory, individual websites could be designated, but this has civil liberties implications and has thus far been avoided due to a significant potential for abuses by governments who might take advantage of such a development to silence political opponents.

Designations are made on the basis of prioritising those members of Daesh or al-Qaeda who are most likely to be exposed to the effects of sanctions. To date, the UN Security Council sanctions committee has been focused primarily on individuals engaged in incitement to violence, but online military training is also prohibited under arms embargoes applied by the committee. Large-scale cyberattacks emanating from Daesh were a possibility in the past, when the group controlled large amounts of territory and had access to substantial material resources. Today, counter-terrorism specialists at the UN anticipate that Daesh's media presence will increase in the wake of their military defeat. This has strategic implications and Daesh may expand its presence in cyberspace, hence the prospect of more proactive engagement by the UN in the future. Daesh apparently still has access to financial assets, but the funds have been laundered into real estate and other concrete investments. Nonetheless, the use of malicious activities such as ransomware attacks to generate additional funds could become a serious problem in the future.

The use of malicious activities such as ransomware attacks to generate additional funds could become a serious problem in the future.

The surge in terrorist attacks and hate crimes by radical right-wing organisations in the US has brought the role of the private sector to the fore. While most of the measures aimed at limiting access to online platforms – such as the suspension of Twitter or Facebook accounts – are based on the violation of the terms and conditions of use, we have recently seen unprecedented steps taken by the private sector. Following the mass shooting in El Paso in August 2019, the discussion about access and use by radical right groups of online services such as anonymous message boards or communication platforms has intensified. As a consequence, 8chan – one such platform which

13 'Hack backs' could be used as exploratory measures, to access services for attribution purposes, as preventive measures, to prevent an actor from doing harm, and as retaliatory measures for revenge. The last aspect is the most debated one.

14 Jacqueline Thomsen, "Pentagon cyber official warns U.S. companies against 'hacking back'", *The Hill*, November 13, 2018. See also: Wyatt Hoffman and Steven Nyikos, "Governing Private Sector Self-Help in Cyberspace: Analogies from the Physical World", *Working Paper*, Carnegie Endowment for International Peace, December 2018, https://carnegieendowment.org/files/Hoffman_Nyikos_Self_Help_FINAL_WEB_bio_edit.pdf; Sven Herpig, "Hackback ist nicht gleich Hackback", *SNV Impuls*, July 24, 2018, https://www.stiftung-nv.de/de/publikation/hackback-ist-nicht-gleich-hackback.

hosted the anti-immigration manifesto of the man accused of the shooting – was taken down by the security company Cloudfare, which decided to no longer provide its services. Tocows, a company that helped register the website, has also withdrawn its support, leaving the message board without a functioning web address.[15] Because websites like 8chan rely on a complex network of internet infrastructure companies, any of such small companies providing essential services (e.g. web addresses, cloud computing power, etc.) can play a critical role in enforcing a regime of cyber-enabled sanctions or *de facto* contribute to establishing such a regime through its self-regulatory practices.

In addition, organisations such as Tech Against Terrorism were created to prevent tech companies whose technology and products are exploited for terrorist activities incurring potential reputational damage. In a similar vein, to curb the spread of terrorist content online, Facebook, Microsoft, Twitter, and YouTube announced in 2017 the formation of the Global Internet Forum to Counter Terrorism. All these companies report significant progress in removing violent extremist content. For instance, between July 2017 and December 2017, a total of 274,460 Twitter accounts were permanently suspended for violations related to the promotion of terrorism. Facebook manages to detect 99% of Daesh and al-Qaeda-related terror content which is removed even before anyone in the forum or community concerned has flagged it. The terrorist attack in New Zealand in 2019 and the announcement of the Christchurch Call to eliminate terrorist and violent extremist content online have further reinforced the norm that the internet should remain a free, open and secure space for all and should not be abused as an arena for malicious cyber activities. Together with the growing focus on election interference, these two objectives might reinvigorate the discussion about cyber sanctions at the UN. Meanwhile, in the absence of progress in the sanctions discussion, some countries have taken unilateral measures. For instance, the UK conducted offensive cyber operations against Daesh terrorists in the Middle East designed to disrupt their ability to carry out attacks, protect British and coalition forces, and cripple Daesh's online propaganda machine.

CONCLUSIONS

Sanctions are a political tool in the hands of governments. But they carry implications – often quite significant – for other actors, in particular in the private sector which needs to ensure compliance with the limitations imposed by governments. In that sense, the cyber sanctions regime put in place by the EU does not bring any new elements as it simply asks the private sector to comply with travel bans and implement asset freezes. However, the role of the private sector, when it comes to cyber sanctions, goes beyond the traditional private-public sector relationship whereby companies and businesses are simply required to comply with the provisions of the regulations. As a matter of fact, in the case of cyber sanctions – as adopted by the EU – this relationship and attendant dependencies are reversed. As this chapter has demonstrated, governments rely on the private sector for forensic and strategic information, thereby turning the security companies into quasi-intelligence services.

In addition to the operational cooperation, private sector actors have taken it upon themselves to shape the normative discussion about responsible behaviour in cyberspace. This move – even though not directly linked to the EU's sanctions regime – might have broad implications for its application. As argued in earlier chapters, sanctions also play a signalling role in relation to the norms that they aim to promote and strengthen. The proliferation of normative initiatives by the private sector provides an additional dimension to the conversation and creates a new context within which sanctions may be implemented, especially if some of these new norms gain universal recognition.

15 Kate Conger and Nathaniel Popper, "Behind the Scenes, 8chan Scrambles to Get Back Online", *New York Times*, August 5, 2019.

Finally, the private sector already plays the role of a sanctioning power in cyberspace. IT companies and social networks have the power to block access or disconnect individuals and entities who do not comply with their terms of reference or other accepted norms. The examples of the fight against cybercrime and terrorist use of the internet illustrate this point.

CHAPTER 8

GALACTIC COLLISION

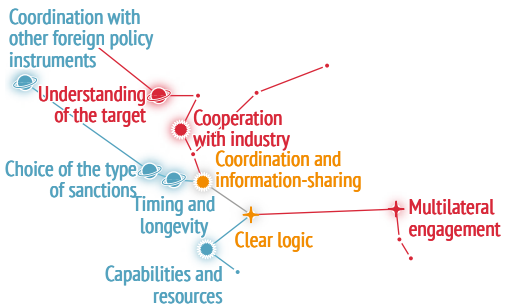
Cyber sanctions and real-world consequences

INTRODUCTION

Astronomers refer to colliding galaxies to describe interactions between different galaxies whose gravitational fields disturb one another. It is not a collision in the traditional sense of the word but rather a stage in the galaxies' evolution that might result in their merger. The existence and functioning of the cyber sanctions regime in parallel to the sanctions regime already put in place and the interaction with other aspects of the real world resembles such a galactic collision.

It is critical for any new cyber sanctions regime to properly identify and address how sanctions affect the cyber world, how the cyber world can favour sanctions evasion, as well as some of the challenges for the cyber world in adapting to existing sanctions. Sanctions have a number of consequences, which can be direct or indirect, as well as intended and unintended. Direct consequences can be produced by the very imposition of sanctions. For instance, an increase in the cost of fuel can be an intended consequence of an oil ban, perhaps to reduce the mobility and autonomy of military vehicles, but an increase in the costs of medicine is typically defined as an unintended consequence of sanctions. At the same time, indirect consequences can affect products/services not mentioned by sanctions. For instance, a ban on oil can contribute to a rise in petroleum costs, which indirectly causes an increase in the prices of foodstuffs and medicines. Additionally, there is the issue of the undesired but inevitable consequences of the adoption of sanctions, known in military terms as 'collateral damage': often, unfortunately, the impact which sanctions have been designed to produce comes with consequences that are indeed undesired, yet unavoidable.

Constellation of issues in this chapter



With this in mind, this chapter discusses aspects that should be taken into account when the cyber sanctions regime is put in place and implemented. Some of the issues addressed in this chapter are of particular importance in the context of listings – a step that the EU has so far not undertaken. But the chapter also touches upon how other sectoral, country-specific or thematic regimes can affect cooperation in the cyber domain and hinder effective responses.

CYBER SANCTIONS AND LAW ENFORCEMENT COOPERATION

In the case of malicious cyber activities conducted from abroad, law enforcement can often only work internationally through the Mutual Legal Assistance Treaties (MLAT). As the investigative police force is typically unable to perform an end-to-end investigation, they must rely on their partners in third countries to help identify the criminal, and take any enforcement action. Such forms of cooperation usually require time in order to ensure that law enforcement agencies operate according to due process principles, including ensuring a high standard of proof for the case to be prosecuted successfully. The fact that evidence or the criminal infrastructure might be located across many jurisdictions complicates the process further. For instance, the Avalanche network used by criminal groups since 2009 for conducting malware, phishing and spam activities was dismantled only in November 2016 after more than four years of global investigative efforts that involved the support of prosecutors and investigators from 30 countries as well as the FBI, Europol and Eurojust.[1]

When there is little or no law enforcement cooperation between countries, the investigating police force's only opportunity to arrest the criminal is when he or she travels outside of their country of residence. International arrest warrants or Red Notices can be issued, but they are not always public, which can give the perpetrators a false sense of security and does not alert them to potential consequences when, for instance, they decide to travel. For example, Russian national Aleksandr Panin, accused of masterminding the SpyEye malware, was arrested while visiting the Dominican Republic.[2] In another example, Vladimir Drinkman, suspected of the theft of credit card numbers from retailer TJ Maxx, was arrested during a trip to the Netherlands.[3] Travel bans, as one type of sanction, thus have the potential of negatively affecting the ability of police forces to arrest criminals and enforce the law. This implies that when discussing possible listings, it is necessary to take into account potential adverse implications for the ongoing criminal investigations and take measures to deconflict both types of instruments. Otherwise, the effectiveness of both the cyber sanctions regime and law enforcement will be undermined.

Sanctions regimes and criminal investigations operate on the basis of a different logic and timeframe .

It is also important to consider how cyber sanctions might affect political relations between states and practical operational law enforcement cooperation. Due to its international nature, cybercrime can often be conducted from unfriendly or sanctioned countries, meaning that criminals are well beyond the reach of law enforcement agencies and making an investigation more difficult. In cases of non-cooperative regimes, indictments or targeted sanctions can be a last resort, but such decisions should be based on an earlier assessment of the potential negative impact on criminal investigations. Recognising that sanctions regimes and criminal investigations operate on the basis of a different logic and timeframe (i.e. political motivation and urgency in the case of sanctions regimes as compared to punitive action and a potentially longer timeframe set by due process requirements),

1 Europol, "'Avalanche' network dismantled in international cyber operation", Press Release, December 1, 2016, https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation.

2 Donna Leger Leinwand and Anna Arutunyan, "How the feds brought down a notorious hacker", *USA Today*, March 5, 2014, https://www.usatoday.com/story/news/2014/03/05/hackers-prowl-dark-web/5982023/.

3 Tom Porter, "'Don't Travel Abroad' Russia warns Hackers", *International Business Times*, July 1, 2014.

there is a need for a reconciliation between the two approaches. While some level of misalignment is unavoidable, especially when the specific crime does not rise to the level of national security significance (in contrast to many sanctions regimes), it is important to look at the whole picture of how specific listings can work in concert with law enforcement measures to punish and prevent criminal behaviour. The effectiveness of this cooperation will depend to a large extent on whether the cyber-criminal under scrutiny is acting in coordination with the government or not.

CYBER TOOLS FOR SANCTIONS EVASION

Another interesting example concerns the interaction between the cyber world and other existing regimes, whereby cyber heists, ransomware attacks and cryptocurrencies have emerged as means to generate funds and undermine country- or sector-specific sanctions already in place.

When access to the international banking system is restricted, some states leverage cyberattacks to gain access to funding. These can involve attacks that both transfer funding through existing banks, but masking them as simple in-person withdrawals, or through cryptocurrency where the transaction may be mapped, but the receiving party is unknown. In February 2016, during an attack on the Bangladesh Central Bank, hackers leveraged and exploited the SWIFT system to transfer money to an account in the Philippines. This and other attacks were linked to North Korea through similarities in code used in otherwise attributed attacks.[4] During the WannaCry ransomware attack in 2017, over £108,000 was taken from three online bitcoin wallets that were advertised to victims for them to retrieve their encrypted data.[5] In 2018, the United States Department of Justice issued a criminal complaint charging North Korean citizen Park Jin Hyok over his involvement in both attacks and connecting him with the North Korean government's malicious cyber activities, including WannaCry.[6] In March 2019, an Expert Panel reported to the UN Security Council on a trend in the DPRK's evasion of financial sanctions 'of using cyberattacks to illegally force the transfer of funds from financial institutions and cryptocurrency exchanges.'[7]

In addition, attention among governments and the private sector is increasingly focusing on ways in which rogue actors are seeking to make use of cryptoassets in an attempt to evade sanctions. Individual, companies and other entities engaged in cryptocurrency transactions are bound by the same sanctions compliance obligations as other traditional financial activities. For instance, on 19 March 2018, US President Trump signed Executive Order EO13827 banning US persons from using any digital currencies linked to the Venezuelan government.[8] In the same month, the US Treasury's Office of Foreign Assets Control (OFAC) stated that all its existing sanctions regimes apply to all US cryptocurrency firms, including those based outside the country that supply cryptocurrency services to US persons. It added that OFAC might start to list cryptocurrency addresses pertaining to companies and individuals that are on US

4 Emma Chanlett-Avery, Liana W. Rosen, John W. Rollins, and Catherine A. Theohary, "North Korean Cyber Capabilities: In Brief", Congressional Research Service, Washington, August 3, 2017.

5 Samuel Gibbs, "Wannacry: hackers withdraw £108,000 of bitcoin ransom", *The Guardian*, August 3, 2017, https://www.theguardian.com/technology/2017/aug/03/wannacry-hackers-withdraw-108000-pounds-bitcoin-ransom.

6 US Department of Justice, "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions", *Justice News*, September 6, 2018, https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

7 Hugh Griffiths *et al.*, "Letter dated 21 February 2019 from the Panel of Experts established pursuant to resolution 1874 (2009) addressed to the President of the Security Council", United Nations Security Council, February 21, 2019, https://undocs.org/S/2019/171.

8 Mark P. Sullivan, "Venezuela: Overview of U.S. Sanctions", Congressional Research Service, Washington, March 8, 2019.

sanctions blacklists.[9] But the decentralised, transnational and anonymous nature of cryptocurrency practices makes it possible for a sanctioned actor to access virtual assets from anywhere in the world without having to make use of the formal banking system. Cryptocurrency firms can engage – knowingly or otherwise – in providing services within sanctioned regimes without such transactions being easily traceable by banks' compliance departments or regulatory authorities. Equally, individuals and firms may be based in a sanctioned regime but mask their location and identity through the use of techniques such as virtual private networks (VPNs), in order to carry out transactions that may be in breach of sanctions. Furthermore, some individuals or firms acting as virtual asset peer-to-peer (P2P) exchangers are able to broker unlicensed transactions on behalf of third parties, which can open the door to money-laundering and other financial activities that might fall under sanctions.[10]

The scale of sanctions evasion based on cryptocurrency payments is not currently well-understood, however. The US Treasury's Financial Crimes Enforcement Network (FinCEN) has warned that countries such as Iran could be using cryptocurrencies to evade sanctions, suggesting that it has been involved in some $3.8 million worth of bitcoin transactions since 2013.[11] It is unclear to what degree this represents an Iranian sanctions evasion strategy and, moreover, the cited figures do not yet amount to a particularly significant sum of money. Nevertheless, some predict that the volumes of funds under question are set to continue to grow over time. Elsewhere, there is concern over efforts in sanctioned states that include Venezuela, Russia and Iran to build blockchain technology that will provide 'sanctions resistance' for their financial industries.[12] In this vein, both Russia and Iran have undergone pilot tests that make use of Hyperledger Fabric – an open source software platform for blockchain systems used by private firms – to create permissioned ledgers. In early 2018, Russia's largest bank, Sberbank, completed a $12 million corporate bond transaction, using the software to settle purchases. Despite US sanctions banning US companies from providing equity financing or debt to the bank, the software itself was not under sanctions.[13]

Compliance with sanctions is a key challenge for those dealing with the cryptoasset world. Banks and other financial institutions are less able to be sure of international sanctions compliance when relying on more traditional screening and due diligence methods. In the case of financial transactions involving traditional currencies, a given bank will typically have a detailed understanding about the transaction, including the name and location of the bank and identities of other parties involved. In contrast, cryptocurrencies are sent between anonymous actors, typically operating under pseudonyms, whereby their locations and identities are often concealed. While some details may be available, for example on public blockchains, data such as names and geographical data are not widely available. This means that there is a risk that these types of transactions may not be prevented by the financial institutions. Consequently, financial institutions are increasingly turning to technological

Compliance with sanctions is a key challenge for those dealing with the cryptoasset world.

9 US Department of the Treasury, "OFAC FAQs: Sanctions Compliance", 2019, https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#559.

10 David Carlisle, "Cryptocurrencies and Sanctions Compliance: A Risk That Can't Be Ignored", *Elliptic*, October 16, 2018, https://www.elliptic.co/our-thinking/cryptocurrencies-sanctions-compliance-a-risk-that-cant-be-ignored.

11 Financial Crimes Enforcement Network, "Advisory on Iran Sanctions", 2019, https://www.fincen.gov/sites/default/files/advisory/2018-10-11/Iran%20Advisory%20FINAL%2.

12 Yaya Fanusie, "Seeking Sanctions Resistance Through Blockchain Technology", *Forbes*, October 11, 2018, p. 1, https://www.forbes.com/sites/yayafanusie/2018/10/11/seeking-sanctions-resistance-through-blockchain-technology/

13 Ibid.

solutions, such as AML software, in order to review blockchain ledgers for activities occurring in sanctioned jurisdictions.[14] In February 2019, the Paris-based global standard setting organisation for countering illicit finance, the Financial Action Task Force (FATF), issued a statement that recognised the need to better mitigate risks linked to virtual asset transactions, particularly in connection with money laundering and terrorist financing.[15] Soon after, in June 2019 FATF adopted and issued an Interpretive Note to Recommendation 15 on New Technologies[16] (INR. 15) followed by the Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.[17]

The EU has not passed specific legislation in relation to cryptocurrencies to date.[18] Regulation over cryptocurrency exchanges currently resides at the individual member state level, where there is a wide range of variation on how each country approaches the matter. Nevertheless, licences and authorisations granted by individual national regulators can 'passport' exchanges, permitting their operation across the entirety of the EU, under one licensing regime.[19] In February 2018, the president of the European Central Bank, Mario Draghi, said that work was underway to develop the Single Supervisory Mechanism in order to identify financial risks presented by virtual assets. In April 2018, the Fifth Money Laundering Directive (5MLD) was agreed by the EU, bringing cryptocurrency-fiat exchanges of currency under the EU's AML legislation and requiring KYC/CDD (Know Your Customer/Client Due Diligence) operations to be carried out on customers in line with normal reporting requirements.[20] The directive brings the EU in line with virtual assets measures introduced by the US some six years ago.[21] In early 2019, the European Banking Authority called for pan-EU rules on virtual assets, arguing that the heterogeneity of approaches to cryptocurrency regulation across the bloc could be open to exploitation.[22] In April 2019, the EU launched the International Association of Trusted Blockchain Applications (INATBA) to further efforts in this area. In a different vein, there is a risk that overregulation of crypto assets and wider digital technologies might undermine some of their potentially positive contributions to humanitarian payments executed in war zones and humanitarian crises.[23]

14 Ibid.

15 Financial Action Taskforce (FATF), "Public Statement – Mitigating Risks from Virtual Assets", February 22, 2019, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html.

16 Financial Action Taskforce (FATF), "Public Statement on Virtual Assets and Related Providers", June 21, 2019, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html.

17 Financial Action Taskforce (FATF), "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers", June 21, 2019, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html.

18 Robby Houben and Alexander Snyers, "Cyrptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion", European Parliament Study, July 2018.

19 "Cryptocurrency Regulations in the EU", *Comply Advantage*, 2019, https://complyadvantage.com/knowledgebase/crypto-regulations/cryptocurrency-regulations-eu-european-union/

20 Tom Robinson, "Inside Analysis on the Latest in Bitcoin, Ethereum & Blockchain", *Elliptic*, May 1, 2018.

21 Ibid.

22 Caroline Binham, "Cryptocurrencies: European Banking Authority calls for Pan-EU Rules on Crypto Assets", *Financial Times*, January 9, 2019.

23 One Danish study argued that digital solutions can help to reduce the time required for humanitarian transactions to clear, reduce bureaucratic costs and curb corruption. See: Jeremy Nation, "Cryptocurrencies as a Vehicle for Humanitarian Aid from Denmark", *ETH News*, December 14, 2017. Their use is also being explored in contexts such as the Syrian conflict, where banking over-compliance, or 'de-risking', complicates financial payments required for the work of humanitarian organisations in the context of complex, overlapping sanctions regimes. See: Justine Walker, "The Foreign Policy Tool of Sanctions, Conflict and Ensuring Continued Access to Finance", *Journal of Financial Crime*, vol. 24, no. 3 (July 2017): pp. 480-90.

SANCTIONS AND INCIDENT RESPONSE COOPERATION

The final example of the 'collision' is the impact of the existing sanctions regimes on cooperation in cyberspace and potentially conflicting norms. Cybersecurity incidents are rarely limited to a single state or economy, which is why international cooperation in crisis management and incident response is a key element. Since the risk factors leading to exploitation are specific to technologies, rather than state-level policies, attacks can easily spread between jurisdictions. In fact, even cyberattacks targeting a single state have had effects outside of the immediate target area. NotPetya was an atypical, destructive malware attack that in 2017 initially propagated through a malicious update for accounting software, M.E.Doc, primarily used in Ukraine. Due to the fact that many multinationals, including international shipping company Maersk, had offices in Ukraine and were required or encouraged to use the software, the attack quickly affected systems outside the physical borders of the country.[24] Stuxnet, a malware which was targeted against the Iranian nuclear programme, was quickly identified on over 200,000 computers in many countries, predominantly Iran, Indonesia and India, but also even in the US, albeit to a lesser extent.[25]

New technologies provide ample opportunities for cyber criminals and sanctioned states to minimise the adverse effects of the sanctions imposed on them.

In such a context, the UNGGE reports and confidence-building measures endorsed by several regional organisations also call upon states to cooperate and provide assistance when so requested by another country or organisation. To facilitate such cooperation and in order to mount an effective response during security incidents, a global community of Incident Response teams, often referred to as Computer Security Incident Response Teams (CSIRTs) or Computer Emergency Response Teams (CERTs) have come into existence.[26] In many ways, the global CSIRT community has always resembled the 'e-SOS system':[27] an international 'duty to assist' norm in which it is required to provide assistance to a victim asking for help, even when it is unknown who is threatening them.

While CSIRTs typically engage and cooperate directly with a peer CSIRT during an incident, they exchange best practices and lessons in these wider communities. Many of these networks do not have formal agreements in place between their members, but are built on a basis of trust, prior cooperation and an understanding that they derive mutual benefits from participation. During a major event, CSIRTs exchange details on the effects of an attack, and best practices on what has worked in their constituency to mitigate an attack. Other CSIRTs apply these lessons to successfully deter an ongoing attack more quickly and avoid repeating mistakes that others in the community may have made. Adversaries gain from a defender's inability to share across borders.

However, the world of the CERT/CSIRT community has been fragmented due to existing sanctions regimes which have made cooperation with countries like Iran, Russia, Sudan or

24 Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

25 Symantec, "W32.Stuxnet. Security Center," September 26, 2017, https://www.symantec.com/security-center/writeup/2010-071400-3123-99.

26 These organisations focus on responding to security incidents within a particular constituency. Corporations often operate a CSIRT as part of their cybersecurity programme. Many states maintain CSIRTs with responsibility over government networks, or even operate, support, or are served by, national CSIRTs, which support citizens within the state during a cyberattack.

27 Duncan Hollis, "An e-SOS for Cyberspace", *Harvard International Law Journal*, vol. 52, pp. 374-430.

Limits to international cooperation: Duqu

In October 2011 Symantec published a report describing Duqu based on a study by the Budapest University of Technology and Economics.* The same month, Kaspersky Labs – a Russian-based developer of anti-malware solutions – published a blog devoted to the same malware and based on a previous investigation conducted in partnership with the Sudanese Computer Emergency Response Team. During their investigation, Kaspersky concluded that the dates of these incidents matched up with the dates that had been originally published by the Iranian authorities who back in April 2011 had identified the Stars malware.** In this case, the challenges to cooperation between different countries were twofold. First, in the wake of the Stuxnet malware, which had previously affected the same Iranian networks, there was little trust between the Iranian cyber defenders who identified the malicious code and the community of incident responders in other parts of the world. Second, Microsoft, as a US-based corporation, was subjected to a sanctions regime administered by the Office of Foreign Assets Control (OFAC) in 2011 against Iran and Sudan where the attack was first identified.*** Based on Executive Order 13059 dating from 19 August 1997, 'the exportation, re-exportation, sale, or supply, directly or indirectly, from the United States, or by a United States person, wherever located, of any goods, technology, or services to Iran' was prohibited. Conversely, the export of services from Iran to the United States is similarly prohibited.**** Even though these and a wide set of other written instructions do have exemptions, they are often hard to decipher due to their limited and complex nature. 'Services' do not necessarily imply the need for a payment, which is illustrated by the fact that general License D-1 embeds a specific exception in the Iran sanctions for communications services which are provided at no cost to the user, implying it would otherwise be covered.***** Given this uncertainty, in the Duqu case, incident responders in the United States were restricted from engaging proactively with incident responders in Iran to effectively assess the risk of the initial malware report from the country in April 2011, which otherwise might have allowed for a more effective handling of the incident.

* Microsoft, "Microsoft Security Advisory 2639658," November 3, 2011, https://docs.microsoft.com/en-us/security-updates/securityadvisories/2011/2639658.

** Aleksandr Gostev, "The Duqu Saga Continues: Enter Mr. B. Jason and TV's Dexter," *Securelist*, November 13, 2011; "Iran target of new cyberattack," *Mehrnews*, April 29, 2011.

*** Government Publishing Office, "31 CFR § 560.509 - Certain transactions related to patents, trademarks, and copyrights authorized. Iranian Transactions and Sanctions Regulations," July 1, 2015, https://www.govinfo.gov/app/details/CFR-2015-title31-vol3/CFR-2015-title31-vol3-sec560-509

**** Department of the Treasury, "Executive Order 13059 of August 19, 1997 Prohibiting Certain Transactions With Respect to Iran," August 19, 1997, https://www.treasury.gov/resource-center/sanctions/Documents/13059.pdf.

***** Department of the Treasury, "Iranian Transactions and Sanctions Regulations. 31 C.F.R. Part 560. General License D-1," February 7, 2014, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/iran_gld1.pdf.

North Korea very difficult. CSIRTs and other partners in this global process are often challenged in working with sanctioned states across two main areas:

1. Trust building: Trust and technical standards that lead to a successful response in a security incident are built as a result of developing cooperative working habits prior to the incident actually unfolding. Because sanctions regimes often restrict these personal interactions, they also restrict the ability of states to set up a successful process for handling incidents, prior to their emergence.

2. Over-compliance/de-risking: as sanctions regimes are often rooted in the goal to reduce economic interaction with a state, they often inadvertently or intentionally generate the perception that all engagement is prohibited. Most attorneys involved in handling

technical cybersecurity challenges are not trained in also ensuring sanctions compliance, and incident responders, at a technical level, will often shy away from engaging with organisations or countries that are located in a sanctioned jurisdiction, regardless of the scope and depth of the actual sanctions in place. While regular engagement may be permitted under the concept of 'general licences' in specific cases of sanctions implementation, cyber 'security' may be listed under dual use or defence-related materials, which creates additional complications.

The constraints on cooperation in the case of a malware named Duqu offers a good illustration of this problem.

CONCLUSIONS

The purpose of this chapter was to investigate how the growing complexity of the relations between existing sanctions regimes and the cyber world might affect the effectiveness of the measures. The interaction between the real and virtual world significantly increases the density of topics and issues that need to be taken into account and therefore makes decision-making more complicated from the technical, legal and operational point of view.

As this chapter has shown, new technologies provide ample opportunities for cyber criminals and sanctioned states to minimise the adverse effects of the sanctions imposed on them. Ransomware attacks or cyber heists have proven to be an effective way for targeted individuals or companies to generate funds while under the asset freeze. They are clearly measures of desperation which on one hand demonstrate that the existing sanctions do bite, while on the other hand exposing their limitations. At the same time, the rapid development of blockchain technologies exemplifies the difficulty for regulators to stay ahead of the curve and ensure that adequate legal measures are in place. From the legal perspective, designing an effective response across the physical and cyber world requires knowledge of regulations addressing technological and compliance aspects. This requires significant investments on the part of the governments, companies and other organisations willing to undertake cooperation – a critical constraint to which cyber criminals and other malicious actors are not subjected. Finally, in clearly operational terms, the rules pertaining to the physical world do not necessarily reflect the realities of the digital space. While rapid transnational cooperation is a quintessential aspect of effective response to cyberattacks and incident handling, the existing rules designed for other policy areas are simply too slow and consequently make cooperation difficult.

CONCLUSIONS

ESCAPING THE BLACK HOLE

Implementation of the EU's cyber sanctions

INTRODUCTION

Establishing a cyber-specific sanctions regime marks another milestone in the EU's efforts to promote responsible behaviour and eradicate impunity in cyberspace. The proposed cyber sanctions regime builds on the EU's previous experiences with horizontal sanctions regimes and other sectoral or country-specific approaches. As explained in the opening chapter, Council Decision 2019/797and Council Regulation 2019/796 of May 2019 established a general framework for the EU's sanctions regime. However, challenges to the implementation of this regime will emerge with the discussion about the first listings. The fact that this is to some extent 'uncharted territory' for the EU does not imply that there is no guidance available. In order to better prepare for the implementation of this regime, the opening chapter of this *Chaillot Paper* has listed ten questions to guide the next steps based on lessons drawn from other sanctions regimes. The following sections discuss what some of those lessons mean in practice.

IS THE LOGIC OF THE SANCTIONS REGIME CLEARLY DEFINED?

The opening paragraphs of the Council Decision and Regulation invoke the European Council Conclusions of 18 October 2018 which called for the EU to develop the capacity to respond to and deter cyberattacks through the imposition of sanctions. Consequently, paragraph 7 of Council Decision 2019/797 establishes a framework for targeted sanctions 'to deter and respond to cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States'. These opening passages make it clear, therefore, that the new cyber sanctions regime is intended to deter and respond to specific instances of cyberattacks. It is sobering to note, however, that research on the effectiveness of UN targeted sanctions has concluded that individual designations, on their own, are rarely effective in coercing, constraining or signalling targets. The effectiveness of targeted sanctions in such cases has been found to be lower unless accompanied by sectoral measures. The current regime, however, does not foresee the adoption of sectoral measures. This option was abandoned for two main reasons. Acknowledging the challenges posed by attribution, the EU member states understood that assigning responsibility for a specific attack or a failure to prevent malicious cyber activities to a third state would inevitably be problematic and would involve high political costs. The choice of individually targeted measures over sectoral measures – at least at this point in time – suggests that member states consider the risk of incurring such political costs as excessively high.

In addition, it would be challenging to combine sectoral and targeted sanctions given the specificity of the latter and the potential counterproductive effect of deciding *a priori* which sectoral

measures to apply. Such sectoral measures can of course be adopted in the future given the Council's wide discretion in deciding on the application of sectoral sanctions and a different (lower) level of substantiation required for such measures. The only limitation in that respect comes from the potential unintended effect of sanctions on the civilian population which the Council needs to take into account. Application of sectoral measures would also have to factor in the principle of proportionality. For instance, in the case of the EU sanctions imposed on Russia over its intervention in Ukraine and annexation of Crimea in 2014, the EU RELEX group engaged in a detailed discussion of the appropriate calibration of the sanctions measures applied to Russia. They were concerned that a disproportionate response by the EU could lead to escalation on the Russian side and the spectre of drastic cuts in oil and gas shipments to EU member states as a retaliatory measure.

Proposal 1

> The European External Action Service and the Council Working Party on Cyber Issues, in cooperation with the RELEX Counsellors group, will play a key role in the implementation of the cyber sanctions regime. To avoid delays in the future, they may consider already ahead of time clarifying various aspects necessary for the successful implementation of the cyber sanctions regime (e.g. developing common understanding of the listing criteria, agreeing on what constitutes a significant attack, etc.), and exploring (i) the possible expansion of the existing sanctions regimes to include cyber-aspects and (ii) the conditions for establishment of a cyber-specific sectoral sanctions regime.

IS COORDINATION WITH OTHER FOREIGN POLICY INSTRUMENTS ENSURED?

Development of a sanctions regime does not take place in a policy vacuum. Like any other decision related to interstate relations, it projects onto and reflects the nature of relationships that a country enjoys with other members of the international community. In order to be effective, the inception and application of a sanctions regime needs to be carefully considered as a tool for conducting foreign and security policy, and tailored to the accomplishment of concrete objectives. The case of the EU cyber sanctions regime is no different.

Deterrence and crafting a response to cyberattacks are clearly listed as the motivation for putting the cyber sanctions regime in place. The Joint Communication 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU' of 13 September 2017 states that 'effective deterrence means putting in place a framework of measures that are both credible and dissuasive for would-be cyber criminals and attackers'.[1] Consequently, the Joint Communication defines concrete measures to support such an approach: (i) identifying malicious actors by improving capacity to identify those responsible for cyberattacks; (ii) stepping up the law enforcement response, including by facilitating cross-border access to electronic evidence, establishing common forensic standards, and promoting the Council of Europe Convention on Cybercrime; (iii) public-private cooperation against cybercrime; (iv) stepping up the political response, including through the implementation of the Cyber Diplomacy Toolbox; and (v) building cybersecurity deterrence through the

1 European Commission, Joint Communication to the European Parliament and the Council, "Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU", *JOIN(2017) 450 final*, Brussels, September 13, 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=ES

member states' defence capability, including concrete cyber defence within the framework of Permanent Structured Cooperation (PESCO) and further integrating cybersecurity and defence into the CSDP. Such an understanding of deterrence, however, suggests that application of the EU sanctions regime needs to be closely coordinated with the criminal law and justice responses. This approach, however, would be too limited and disregard a vast range of other foreign policy instruments at the EU's disposal.

An additional challenge for the application of the EU's cyber sanctions regime stems from the rather vague nature of the concept of deterrence and how it might apply to cyberspace. The existing scholarship investigates whether conventional or nuclear models of deterrence are applicable to cyberspace, and whether deterrence by punishment or denial, or some combination thereof, works better given the particularities of the cyber domain.[2] It is useful to stress, however, that deterrence effectiveness remains an elusive concept, with no widely accepted causal model of deterrence to draw on in cyber because, *inter alia*, in deterrence there are always too many variables at play.[3] There is, in other words, no consensus on what policies, acts and practices actually carry a deterrent effect in cyberspace.[4] That also means that the deterrent effect of the EU's cyber sanctions may prove difficult to monitor and measure, likely leading to its failure as an objective.

Proposal 2

> In the absence of a unified EU member states' position regarding deterrence in cyberspace, the EEAS together with the Presidency of the Council play an important role in forging a better understanding among the EU member states and working towards a common appreciation of the importance of this concept in the EU context. This requires mapping concrete policy instruments that would fall under the EU's 'cyber deterrence framework', in particular regarding the linkages between cyber sanctions and other policy instruments. In this context, it will be particularly important to clarify and develop a common understanding regarding the activation of the solidarity clause (art. 222 TFEU) and mutual defence clause (art. 42.7 TEU) in response to a cyberattack.

Proposal 3

> In order to ensure that the broader foreign and security policy implications are taken into account, the Political and Security Committee (PSC) as well as the COREPER representatives will require a more detailed understanding of cyber-related issues in order to ensure a more joined-up and comprehensive response by the EU. Therefore, the already conducted 'table-top exercises' involving different EU institutions and the member states could increasingly expand to include other actors in order to make sure that the joined-up approach to cyber issues is adequately operationalised.

DO THE CHOSEN SANCTIONS SUPPORT THE STATED OBJECTIVES?

The EU's cyber sanctions regime foresees two types of measures: travel bans and freezing assets. These measures are intended to be used against natural or legal persons, entities or bodies that are responsible for cyberattacks or

2 Joseph Nye, "Deterrence and Dissuasion in Cyberspace", *International Security*, vol. 41 , no. 3 (2017): pp.44-71,.

3 Lawrence Freedman, *Detterence* (Cambridge: Cambridge University Press, 2004).

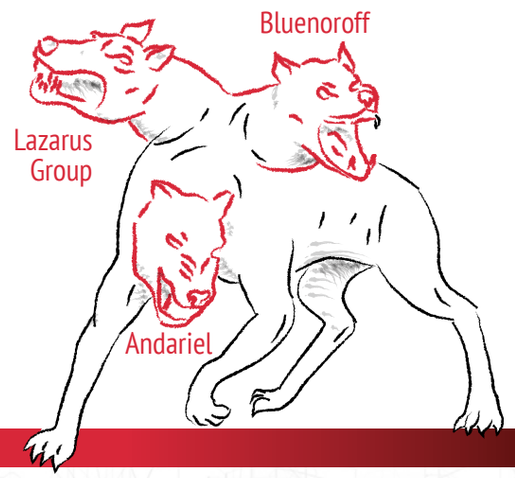
4 The authors are grateful to Xymena Kurowska for this observation.

How do sanctions come to life?

The case of Lazarus Group

In September 2019, the US OFAC announced sanctions targeting three North Korean state-sponsored groups: Lazarus Group (also known as Guardians of Peace or Hidden Cobra), Bluenoroff, and Andariel.

The graphic below shows various stages that led to this decision and the elements that could potentially contribute to a similar decision by the EU.



OPERATIONS AND EFFECTS

Lazarus Group

WannaCry 2.0 ransomware that affected at least **150 countries** around the world and shut down approximately 300,000 computers.

Publicly attributed to North Korea by the United States, Australia, Canada, New Zealand and the United Kingdom in December 2017. Denmark and Japan issued supporting statements.

Bluenoroff

Attacks on financial institutions in Bangladesh, India, Mexico, Pakistan, Philippines, South Korea, Taiwan, Turkey, Chile, and Vietnam.

Operations targeting more than 16 organisations across 11 countries, including the **SWIFT messaging system, financial institutions, and cryptocurrency exchanges.**

Worked with Lazarus Group to steal approximately **$80 million dollars** from the Central Bank of Bangladesh's New York Federal Reserve account.

Andariel

Cyber operations on **foreign businesses, government agencies, financial services infrastructure, private corporations, and businesses, as well as the defence industry.**

Malicious cyber activity against South Korea government personnel and the South Korean military in an effort to gather intelligence.

STATE RESPONSIBILITY

Created by the North Korean Government as early as 2007, Lazarus Group is subordinate to the 110th Research Centre, 3rd Bureau of the Reconnaissance General Bureau (RGB).

The 3rd Bureau is also known as the 3rd Technical Surveillance Bureau responsible for North Korea's cyber operations. The RGB is also involved in the arms trade.

The UN also designated the RGB on March 2, 2016.

NORM VIOLATIONS

Attacks against institutions performing **key societal functions**, such as government, military, financial, manufacturing as well as **critical infrastructure**, using tactics such as cyber espionage, data theft, monetary heists, and destructive malware operations.

Malicious cyber activity against foreign financial institutions to **earn revenue illicitly in response to increased global sanctions**, in part, to fund the North Korean **nuclear weapons and ballistic missile programmes**, in violation of the UN sanctions.

Bluenoroff cyber operations also target Virtual Asset Providers and cryptocurrency exchanges to possibly assist in obfuscating revenue streams and cyber-enabled thefts. Lazarus Group, Bluenoroff and Andariel likely stole around **$571 million in cryptocurrency** alone, from five stock exchanges in Asia between January 2017 and September 2018.

INDICTMENT

In June 2018, the FBI issued a federal arrest warrant for **Park Jin Hyok** – a North Korean programmer, member of the Lazarus Group and employee of a government-owned company, Chosun Expo Joint Venture. These were followed by the formal charges in September 2018.

Park is accused of participating in the **WannaCry** attack, the 2016 Bangladesh Central Bank cyber-heist, attempts at hacking US defence contractor **Lockheed Martin** in 2016, and the 2014 **Sony Pictures** hack, among others.

The US Department of the Treasury has **also imposed sanctions** on Park and Chosun Expo.

SANCTIONS

Evidence

Primarily open source information from security companies (e.g. FireEye, Kaspersky, Symantec and MITRE).

In addition, the US Cybersecurity and Infrastructure Security Agency (CISA) and Cyber Command (USCYBERCOM) disclosed malware samples to the private cybersecurity industry, several of which were later attributed to North Korean cyber actors.

Decision

Treasury took action against the use of cyberattacks against critical infrastructure and to support North Korea's illicit weapon and missile programmes.

Measures

All property and interests in property of these entities, and of any entities that are owned, directly or indirectly, are blocked and must be reported to OFAC.

Persons that engage in certain transactions with the designated entities may themselves be exposed to designation.

Any foreign financial institution that knowingly facilitates a significant transaction or provides significant financial services for any of these entities could be subject to US sanctions.

Strategic Communication

Press release stating all the facts and rationale for sanctions.

attempted cyberattacks as well as any person or organisation that provides financial, technical or material support for such activities (including by planning, participating in, directing, assisting or encouraging such attacks, or facilitating them by action or omission). While the regimes's scope is quite broad and targeted at an extensive group of actors – whose calculus about engaging in prohibited activities might change over time– there is a more general question whether such measures will have an impact beyond individuals. Past experiences show that in most cases of significant cyberattacks there was a clear link to a state. The question, therefore, is whether targeted individual sanctions are capable of changing state behaviour.

At the same time, the preamble to the Council Decision insists on a clear differentiation between targeted restrictive measures and the attribution of responsibility for cyberattacks to a third state. The document argues that targeted sanctions do not amount to such attribution, which is a sovereign political decision taken on a case-by-case basis. Such a distinction might be politically convenient for the EU and its member states, as it precludes any accusation of assigning political responsibility to another state, hence avoiding any potential damage to bilateral relations. In practice, however, such a neat separation between targeted sanctions and attribution might be difficult to maintain. This also points to a paradox whereby the EU measures aim to deter and change state behaviour without making an explicit link to the states concerned. Such an approach denies an important signalling role that the EU's cyber sanctions regime could play. Except in rare cases, individuals and entities listed by the EU will be nationals or entities based in the territory of a third state, which will undoubtedly attract attention towards that specific state. Within the context of the EU's horizontal regime of restrictive measures against the use and proliferation of chemical weapons adopted on 15 October 2018, the Council designated two GRU officials and the Head and Deputy Head of the GRU as being responsible for the possession, transport and use of a toxic nerve agent in Salisbury (UK) on the weekend of 4 March 2018. Despite being styled as targeted sanctions, this step prompted a reaction from the Russian government who denied any such allegations.

Proposal 4

> While acknowledging the fact that attribution is a sovereign decision of the member states, it is critical that member states in the Council, with the support of the EU INTCEN, work towards establishing minimum standards for a joint or coordinated attribution in order to strengthen the signalling dimension of sanctions – a cyber version of a 'duck test' or 'elephant test'[5] reflecting the evolving knowledge and capacity to attribute.

IS THEIR TIMING AND LONGEVITY ADEQUATE?

Timespan and the speed with which sanctions are enacted tends to affect their effectiveness. As such, sanctions regimes should be designed to be flexible and they should be reviewed and regularly adapted to changing conditions. Council Decision 2019/797 foresees regular reviews – stipulating renewal or amendment as appropriate – if the Council deems that its objectives have not been met. In addition, Council Regulation 2019/796 allows the possibility of reviewing – and amending, if necessary – the listings in Annex I to the Regulation in cases where observations or substantial new evidence is presented. In addition, the list should be reviewed at regular intervals and at least

5 The duck test is usually expressed as 'If it looks like a duck, swims like a duck, and quacks like a duck, then it probably is a duck'. The elephant test refers to situations in which an idea or thing is hard to describe, but instantly recognisable when spotted. Most technical attributions conform to the duck test.

every 12 months. These provisions are very important in light of the evolving capacity to attribute attacks to specific actors. In the past, we have seen several examples of wrongful or multiple attributions. For instance, Olympic Destroyer – a malware associated with attacks during the 2018 PyeongChang Winter Olympics – was simultaneously attributed by different cybersecurity researchers to North Korea, Russia and China.[6]

Another important aspect is the speed at which concrete decisions about listings are taken. The decisions to establish and amend the list set out in the Annex to Council Decision 2019/797 need to be taken by the Council acting unanimously upon a proposal from a member state or from the High Representative of the European Union for Foreign Affairs and Security Policy. Given the sensitivity of the issue, it is very unlikely that such decisions will be enacted quickly and without warning to the target, which will reduce the chances of success by allowing the target time to prepare alternative courses of action.

Proposal 5

> If the likelihood of impact on the target is relatively low – given the lengthy decision-making procedures in the EU – the stated policy objectives might be better served through alternative means, including pursuing a law enforcement approach. It is therefore important that such a cost-benefit analysis is performed each time before the decisions about listings are made. In that sense, the sequencing of sanctions together with other policy instruments needs to be carefully factored in.

DO THEY DEMONSTRATE A DETAILED UNDERSTANDING OF THE TARGET?

The EU cyber sanctions regime is clearly the outcome of the political imperative 'to do something' about the threats emanating from cyberspace and the need to reach compromise among all EU member states. By focusing on individuals and entities as targets of the sanctions, the EU has acknowledged that individuals and non-state actors – including state proxies – pose a serious threat to the security and interests of the EU. In that sense, the EU is following the US approach to cyber sanctions that also targets individuals, albeit with a limited effect to date. This is primarily due to the fact that in most cases those individuals are harboured or supported by a state. At the same time, however, the absence of sectoral or country-specific sanctions shows that the EU is trying to avoid the more politically sensitive question about attribution of responsibility to states. Such an approach has its merits as sanctions may place the relationship with the targeted country on a path towards escalation and conflict, which the EU may want to avoid. Therefore, there is a clear need to think about maintaining dialogue and undertaking confidence-building measures, as well as developing de-escalatory approaches and exit strategies. Interestingly enough, the Council Decision foresees exemptions to that effect by allowing the possibility to travel on grounds of 'attending intergovernmental meetings or meetings promoted or hosted by the Union, or hosted by a member state holding the Chairmanship in office of the OSCE, where a political dialogue is conducted that directly promotes the policy objectives of restrictive measures, including security and stability in

6 See for instance: Andy Greenberg, "'Olympic Destroyer' Malware Hit Pyeongchang Ahead of Opening Ceremony", *Wired*, December 2, 2018, https://www.wired.com/story/olympic-destroyer-malware-pyeongchang-opening-ceremony.

cyberspace'.[7] The focus on the OSCE is noteworthy as it is one of the few remaining platforms for dialogue between the EU and Russia.

At the same time, it is important that the discussion about cyber sanctions takes into account potential adverse effects that it might have on other communities. The exchange of cybersecurity information, such as malicious code for investigation, or best practices to defend against a specific cyberattack and related communications, do not clearly fit into existing exemptions. This is relevant since during an incident, there typically is not sufficient time to apply for a specific licence. The initial outbreak of WannaCry, from when it was unleashed on 12 May 2017 up to the time when a kill switch – a domain which, once registered, stopped the attack – was identified that prevented further harm, took only a few hours.[8] While patches for supported platforms had already been available, Microsoft released additional security updates for unsupported systems on 12 May, the same day as the outbreak occurred. Decisions on how to respond to a major attack effectively often need to be made within hours, not days. The benefits of permitting defensive cybersecurity-related exchanges would most resemble those pertaining to exemptions for medical supplies covered under a general licence. Exchanging information on cyberattacks can improve the safety both of individuals and organisations within the sanctioned state, and those in other countries. This is especially the case if vulnerabilities are exploited first within the sanctioned state. There is some risk involved in sharing information with countries where there may be little legal relief if the information is abused. However, the defensive community already has processes (such as the Traffic Light Protocol, trust mechanisms and international cooperation organisations and tools) in place to prevent excessive disclosure. While these mechanisms can be improved, the community is at greater harm from not being able to respond to an attack due to lack of information, than from the risk incurred by sharing of information on attacks which are already ongoing.

Proposal 6

> To further improve its understanding of the potential targets but also to reduce the risk of escalation, there is a clear need for further investment in the implementation of the confidence-building measures among the EU member states – through the implementation of the NIS Directive, for instance – but also in other regional organisations such as in the OSCE and ASEAN Regional Forum. While new political initiatives with countries such as Russia, China or Iran are often difficult to implement for political reasons, such processes could be supported through track 2.0 initiatives at the expert level, including between academics and researchers.

Proposal 7

> Spill-overs from the cyber sanctions regime might have a significant impact on other policy areas. Consideration should be given to how to coordinate the implementation of sanctions across other branches of the government, such as law enforcement and financial regulators. For example, a measured tradeoff calculation should be made on the impact on open law enforcement investigations when implementing a travel ban. In addition, coordination across the banking system will be important, particularly to detect financial transactions being conducted outside conventional banking channels and to address the challenge posed by alternative remittance systems. Finally, a general licence exemption for first responders (such as members of FIRST) to share defensive cybersecurity information would

7 "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States", *op. cit.*, Article 4, para. 6.

8 Symantec,"Wannacry Timeline", May 24, 2017, https://www.symantec.com/security_response/writeup.jsp%3Fdocid%3D2017-051310-3522-99.

improve their ability to respond effectively to cross-border cybersecurity incidents.

ARE CAPABILITIES AND RESOURCES SUFFICIENT?

As stated earlier, considerable expertise, investment and capabilities are necessary in the efficient imposition, enforcement and monitoring of sanctions. This is likely to be particularly the case in the highly technical and fast-changing cyber domain. With the adoption of the EU cyber sanctions regime, the EU and the member states have a new tool at their disposal. This decision – with significant implications for the existing workload of officials dealing with those issues – has not triggered additional investment in human or intelligence resources within the EEAS. This may be ascribed to the fact that the perception of threat is not shared equally across the different member states and, therefore, willingness to commit resources to tackle this challenge may be shared to a lesser degree than public statements might indicate. This ultimately leads to different levels of capacity among the member states and may affect the implementation of the cyber sanctions regime altogether.

It is not a secret that currently only a handful of countries have the capacity to attribute attacks and share evidence, notably the UK, the Netherlands, France and Estonia who have publicly acknowledged such capacities. The remaining countries either rely on information provided by the private sector or obtained through bilateral contacts with other member states and partners worldwide. The question of capacities is also pertinent regarding the legal capabilities of each member state to assess the legal options available to them and the consequences of each course of action from the international law perspective. As seen also in other sanctions regimes, further integration at the EU level would contribute to sanctions regimes that are more effective (augmented with more personnel and better coordinated) and efficient (with less duplication of the same functions), especially when the technical capacities required are becoming increasingly essential.

Proposal 8

> The existing gaps in technical capabilities and human expertise in the domains of open-source intelligence collection and analysis, forensic capabilities, and application of international law in cyberspace can be easily remedied through additional funding via European Commission programmes and initiatives. Other EU bodies and agencies, including the European Defence Agency (EDA), European Union Institute for Security Studies (EUISS) and European Security and Defence College (ESDC) play an important role in contributing to the development of such capacities.

DO COORDINATION AND INFORMATION-SHARING WORK?

The willingness of the member states to take the political risks associated with the imposition of cyber sanctions will depend to a great extent on their confidence in attribution and/or the supporting evidence. Currently, each member state assesses the information in its possession based on its own resources and methodology. While all countries have acknowledged difficulties in attribution, there is also a recognition that current methods allow for establishing the perpetrators of cyberattacks with high levels of certainty. Given the potentially damaging impact of wrongful attributions on the EU's reputation and credibility, it is not surprising that such evidence is usually carefully weighed. In order to convince all member states to jeopardise their political capital and relations with a third country whose nationals, companies or other entities might be sanctioned by the EU,

a member state or the High Representative for Foreign Affairs and Security Policy will need to present the evidence confirming the link with the conducted or attempted cyberattack. The decisions about sharing potentially sensitive information as well as about trusting the presented information will be a litmus test for the maturity of cooperation between the member states. But it will also require serious investment on the part of the intelligence community in honing their diplomatic skills not only to be able to make a convincing case, but also to decide what type of information to share and with whom. This might be achieved through closer cooperation with the law enforcement agencies and CERTs.

Proposal 9

> In order to strengthen trust among the member states and promote the culture of information sharing, the EEAS and Council can make better use of and promote the existing tools (e.g. IPCR web platform, more targeted CERT-EU reports, and special Cyber Situational Reports by EU INTCEN).

HOW ARE MULTILATERAL ENGAGEMENT AND COORDINATION ENSURED?

Engagement with international partners is relevant in the context of the EU's cyber sanctions for two main reasons. First, the Council Decision and Regulation foresee the possibility of adopting sanctions in support of the third country or international organisation that has been targeted by an attack. It is, therefore, important that the EU has a good situational awareness concerning the vulnerabilities and threats that those countries face. Second, in order to maximise the impact of the EU's cyber sanctions, the EU should encourage third states to adopt sanctions similar to those adopted by the EU. To date, eight countries have aligned themselves with Council Decision 2019/797: the candidate countries Albania, North Macedonia, Montenegro, and Serbia – the countries of the Stabilisation and Association Process – and potential candidate Bosnia and Herzegovina; and the European Free Trade Association (EFTA) countries Iceland and Norway, who are also members of the European Economic Area (EEA), as well as Georgia. However, where the EU autonomous sanctions have had the biggest impact has been when other big economies such as Japan, Canada or Australia have taken a similar approach. Finally, multilateral engagement is key for information exchange and evidence gathering. To date, most of the information has been shared by individual member states working with their counterparts across the world. In some cases, such cooperation has resulted in coordinated attribution by some member states and partner countries (e.g. in response to the WannaCry attack). In this context, it is also important for the EU to gain a better understanding of doctrines and instruments used by partner countries and international organisations, in particular NATO, and their implications for the EU's sanctions regime. The US, for instance, has adopted a far-reaching doctrine of 'persistent engagement' and 'defend forward' which, if conducted without the authorisation of a member state whose cyberspace is being used for such operations, may provide the grounds for cyber sanctions by the EU member states.

Proposal 10

> Dialogues with partner countries and international organisations are essential to better understand different priorities and perspectives. The EEAS could further facilitate these processes through the existing or new bilateral cyber dialogues with key partners (e.g. with Singapore, Australia, South Africa, Kenya and Ghana) and regional organisations (e.g. the Organisation of American States, the African Union) as well as through

more targeted meetings with representatives from those countries in the Council Working Party on Cyber Issues or the PSC.

Proposal 11

> The EU is already one of the biggest spenders when it comes to cyber capacity-building projects in third countries as well as projects promoting better understanding of EU policies among partner countries and international and regional organisations. However, financial commitment should not be mistaken for political engagement. Cyber diplomacy cannot be outsourced to the organisations and institutions implementing the EU-funded projects. There is therefore ample scope for boosting the EU's presence and visibility in the cyber arena.

ARE MECHANISMS FOR COOPERATION WITH INDUSTRY IN PLACE?

The EU cyber sanctions regime does not include any specific provisions concerning cooperation with industry and the private sector, other than in their role as actors required to comply with the adopted measures. However, as this *Chaillot Paper* has shown, there is a more extensive role for the private sector, including as a norm entrepreneur drawing the lines of what is and what is not responsible behaviour in cyberspace as well as providing intelligence and evidence required for listings.

While cooperation with the private sector is necessary, there are several challenges of legitimacy, transparency and accountability linked to public-private cooperation in this domain. The role of private sector actors as norm entrepreneurs raises an obvious question about the legitimacy of such initiatives. Unlike governments, private sector companies are primarily concerned with making a profit. What is also problematic is the fact that most of the companies currently participating in the debates about peace and security in cyberspace are primarily based in the US or in the EU, which raises the question of their global representativeness. For instance, Russia has complained about the exclusion of Russian companies from the Microsoft initiatives, while at the same time stressing similar initiatives by its own companies, including the Charter spearheaded by Nornickel, Russia's leading metals and mining company.[9] This, however, does not diminish the importance of these initiatives in terms of identifying additional norms, setting agendas and raising awareness across different policy communities.

Linked to legitimacy is the question of transparency of policies and practices that private sector companies adopt in their relations with government agencies. This question is particularly pertinent in the case of attribution which might have significant implications for interstate relations and numerous businesses in the EU and third countries. As already indicated, most of the private cybersecurity companies are American and European, which has raised questions about their political motivation and close links to the governments in the US and EU member states. Some of the private security companies have also admitted in the past to having been more circumspect about publishing information about US or allied-linked cyber operations. In an interview given to *Cyberscoop*, a former CrowdStrike employee admitted that the company decided that blogging about such operations before anyone else was 'not an advantageous thing to do'. [10] Similarly, FireEye had drawn a red line regarding the exposure

9 In 2018, Nornickel presented a Charter at the 12th International Forum "Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security" held in Garmisch-Partenkirchen (Germany).

10 Chris Bing, "In the Opaque World of Government Hacking, Private Firms Grapple with Allegiances", *Cyberscoop*, July 23, 2018.

of certain activities by so-called 'friendlies'. In another interview for Mashable in 2014, Ronald Prins, the founder of Dutch security firm FoxIT, admitted that his company chose not to publish details about a malware variant known as Regin due to potential interference with NSA/GCHQ operations.[11]

Another important aspect is accountability.[12] With the increasing reliance on private sector companies for performing state or state-like functions in enforcing cyber sanctions or cyber-enabled sanctions, the lines surrounding the ultimate responsibility for the effectiveness of measures or mistaken decisions made on the basis of wrong information are also blurred. At the same time, the complexity resulting from the dependencies built into the internet infrastructure implies that some of the operations can be error prone, and even put other internet users at risk. Botnet takedowns, albeit very useful for disarming criminal networks, can incur collateral damage, for instance when infrastructure used by the botnet is also used for legitimate purposes, such as in the case of Changzhou Bei Te Kang Mu Software Technology Co Ltd, a Chinese company operating infrastructure leveraged by the Nitol botnet.[13] A vulnerability identified and used to exploit a criminal's system could also be discovered due to a leak, or during use, and re-used in more conventional cybercrime. The vulnerability exploited by the WannaCry ransomware was originally released by a group called The Shadow Brokers, and reportedly stolen from the US National Security Agency (NSA).[14] Partly in an effort to mitigate these risks, or at least to control them, several states have introduced so-called vulnerability equities processes, which prescribe the procedures guiding a decision whether to disclose a discovered vulnerability to the software vendor, or 'stockpile' it for use in these types of operations.

Proposal 12

> The EEAS could consider various possibilities for establishing more formal, transparent and accountable mechanisms for cooperation with the private sector. Several existing models within the member states and other organisations could serve as inspiration. For instance, the Council Working Party on Cyber Issues could be used for more regular dialogue with private sector and sharing good practices among the member states. In addition, to ensure security of its equipment and networks, the EU could draw from its experience with the authorised economic operators (AEOs) and consider establishing an authorised cyber operator (ACOs) scheme, for instance building on the certification and standardisation work of the EU Cybersecurity Agency.

IS THERE A CLEAR COMMUNICATION STRATEGY?

As stated on numerous occasions throughout this *Chaillot Paper*, the success of the EU's cyber sanctions regime – as an instrument of deterrence but also as the means to demonstrate the EU's role as an important player in the cyber domain – will depend on managing expectations and communicating clearly with the outside world. The challenges in this respect are threefold. First, the EU will need to do a better job in explaining its position whereby listings are not equivalent to attribution. While the formal explanation might help internally

11 Lorenzo Franceschi-Bicchierai, "What we know about Regin, the powerful malware that could be the work of NSA", *Mashable*, November 25, 2014, https://mashable.com/2014/11/25/regin-spy-malware-nsa-gchq/?europe=true.

12 Jacqueline Eggenschwiler, "Accountability Challenges Confronting Cyberspace Governance", *Internet Policy Review*, vol. 6, no. 3, September 2017.

13 Suresh Ramasubramanian, "Microsoft's Takedown of 3322.org – A Gigantic Self Goal?", *CircleID: Blogs*, September 2012, http://www.circleid.com/posts/20120917_microsoft_takedown_of_3322_org_a_gigantic_self_goal/

14 Lily Hay Newman, "The Leaked NSA Spy Tool that Hacked the World", *Wired*, March 7, 2018, https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/

in order to avoid lengthy discussions about the division of competences within the EU, it will not be clear to the outside world. Second, the EU's strategic communications should also take into account the role that disinformation in both traditional and social media is increasingly playing in seeking to misrepresent the objectives and impacts of sanctions imposed for political ends, as documented by the Disinformation Review of the EEAS's East Stratcom Task Force. Finally, given the unique nature of cyberattacks, at times committed by an isolated individual, the proportionality of response will be an especially sensitive topic. Imposing sanctions on single issue 'hacktivist' groups, such as those working to tackle climate change or in support of transparency, will be similarly contentious given that this might involve a clash with other EU policies.

Proposal 13

> Sanctions require a clear communication strategy. To promote a better understanding of the EU's cyber policies – not only sanctions – the EEAS, through its delegations but also in close cooperation with the member states, could consider developing a clear communication strategy supplemented with concrete procedures. For instance, any future decisions about listings could be accompanied by a communication plan that not only explains the rationale for the decisions taken by the EU, but also debunks any disinformation about the adopted approach.

ABBREVIATIONS

APT
Advanced Persistent Threat

ASEAN
Association of Southeast Asian Nations

BRICS
Brazil, Russia, India, China and South Africa

C&C
Command and Control

CDT
Cyber Diplomacy Toolbox

CERTs
Computer Emergency Response Teams

CFSP
Common Foreign and Security Policy

COAFR
Africa Working Party

COASI
Asia-Oceania Working Party

COREPER
Committee of Permanent Representatives

CSDP
Common Security and Defence Policy

CSIRTs
Computer Security Incident Response Teams

DDoS
Distributed Denial of Service

DNC
Democratic National Committee

DPRK
Democratic People's Republic of Korea

EC3
European Cybercrime Centre

EDA
European Defence Agency

EEA
European Economic Area

EEAS
European External Action Service

EFTA
European Free Trade Association

ENISA
European Union Agency for Cybersecurity

ESDC
European Security and Defence College

EU INTCEN
EU Intelligence Analysis Centre

FAC
Foreign Affairs Council

FATF
Financial Action Task Force

FBI
Federal Bureau of Investigation

FIRST
Forum of Incident Response and Security Teams

GAC
General Affairs Council

GCHQ
Government Communications Headquarters

GDPR
General Data Protection Regulation

GRU
Main Intelligence Directorate of the General Staff of the Russian Armed Forces

HR/VP
High Representative of the Union for Foreign Affairs and Security Policy/Vice-President of the European Commission

ICJ
International Court of Justice

ICT
Information and Communications Technology

IT
Information Technology

JCPOA
Joint Comprehensive Plan of Action

NATO
North Atlantic Treaty Organisation

NCSC
National Cyber Security Centre

NIS
Network and Information Security

NSA
National Security Agency

OAS
Organisation of American States

OEWG
Open-Ended Working Group

OFAC
Office of Foreign Assets Control

OPCW
Organisation for the Prohibition of Chemical Weapons

OSCE
Organisation for Security and Cooperation in Europe

PESCO
Permanent Structured Cooperation

PLA
People's Liberation Army

PSC
Political and Security Committee

QMV
Qualified Majority Voting

RELEX
Working Party of Foreign Relations Counsellors

SCO
Shanghai Cooperation Organisation

TEU
Treaty on European Union

TFEU
Treaty on the Functioning of the European Union

TSC
Targeted Sanctions Consortium

UN
United Nations

UNDP
United Nations Development Programme

UNGGE
United Nations Group of Governmental Experts

UNSC
United Nations Security Council

WTO
World Trade Organisation

NOTES ON THE CONTRIBUTORS

Karine Bannelier is Associate Professor of International Law and Deputy Director of the Grenoble Alpes Cyber Security Institute. Her recent publications include the book *Cyber-Attacks – Prevention-Reaction: The Role of States and Private Actors* (with T. Christakis, *Revue Defénse Nationale*, 2017); "Obligations de due diligence dans le cyberspace: Qui a peur de la Cyber-Diligence?" (RBDI, 2017); "Rien que la Lex Lata? Etude critique du Manuel de Tallinn 2.0 sur le droit international applicable aux cyber-opérations" (AFDI, 2018). She obtained her PhD in International Law from the University of Paris-Sorbonne.

Thomas Biersteker is Gasteyger Professor of International Security and Director of Policy Research at the Graduate Institute, Geneva. His current research focuses on targeted sanctions, transnational policy networks in global security governance, and the dialectics of world orders. He was the principal developer of SanctionsApp, a tool for mobile devices created in 2013 to increase access to information about targeted sanctions at the UN. He received his PhD and MS from MIT and his BA from the University of Chicago.

Nikolay Bozhkov is a trainee at the NATO's cyber defence section and a former trainee at the EU Institute for Security Studies. At the Institute, he provided research support for the work of the EUISS Task Force on Cyber Sanctions and coordinated its activities. In the framework of the EU Cyber Direct Project, he was closely involved in research on international law and norms in cyberspace as well as on China's digital policies. He obtained his Master's degree in International Security from Sciences Po in Paris with a specialisation in Chinese Studies and Research Methods.

François Delerue is a research fellow in cyberdefence and international law at the French Institute for Strategic Research (IRSEM). His research concerns cyberdefence and cybersecurity, specifically their legal, policy and strategic dimensions. In his research he focuses on international law obligations, norms and international cooperation, as well as on the various actors involved in this area, including states, private companies, and non-governmental organisations. His book, *Cyber Operations and International Law*, is forthcoming from Cambridge University Press. He obtained his PhD from the European University Institute in Florence.

Francesco Giumelli is Associate Professor in the Department of International Relations and International Organization at the University of Groningen. He was previously Jean Monnet Fellow at the European University Institute and Fellow at the Kroc Institute of Notre Dame University. He is the author of *The Success of Sanctions: Lessons Learned from the EU Experience* (Routledge, 2013) and *Coercing, Constraining and Signalling: Explaining UN and EU Sanctions After the Cold War* (ECPR Press, 2011). He has published articles on sanctions, private military and security companies. Beyond his work on sanctions, he studies issues concerning the role of private actors in security and illicit trade. He holds a Ph.D. in Political Science from the Institute for Humanities and the Social Sciences.

Erica Moret is Senior Researcher at the Centre for Global Governance at the Graduate Institute of International and Development Studies, Geneva, and chairs the Geneva International Sanctions Network (GISN). She holds a DPhil (PhD) and MSc from the University of Oxford and is also a graduate of the Ecole Nationale d'Administration (ENA) in Paris. She has written extensively on European foreign and

security policy and sanctions, and in relation to cybersecurity, Brexit and informal governance. She heads the 'Compliance Dialogue on Syria-Related Humanitarian Payments' on behalf of the Swiss government and the EU's DG ECHO and has advised the UN's Office for the High Commissioner on Human Rights. She regularly participates in task forces on sanctions and European security for the EU, UN and European governments.

Patryk Pawlak is the EUISS Brussels Executive Officer. In this capacity, he maintains and develops relations with other Brussels-based institutions. In addition, he is in charge of the cyber portfolio, leading the Institute's cyber-related projects and contributing to its outreach activities. He is currently Project Coordinator for EU Cyber Direct – an EU-funded project focused on supporting the EU's cyber diplomacy. He is also a Co-Chair of the Advisory Board of the Global Forum on Cyber Expertise. His current work focuses on the interplay between international law, norms and capacity building in cyberspace. He holds a PhD in Political Science from the European University Institute in Florence and an MA in European Studies from the College of Europe.

Maarten Van Horenbeeck is Chief Information Security Officer at Zendesk and a Board Member and former Chairman of the Forum of Incident Response and Security Teams (FIRST). Prior to working at Zendesk, he was Vice President of Security Engineering at Fastly and worked on the security teams at Amazon, Google and Microsoft. He holds a Master's Degree in Information Security from Edith Cowan University and a Master's Degree in International Relations from the Freie Universität Berlin. He is a fellow in New America's Cybersecurity Initiative, and lead expert to the IGF's Best Practices Forum on Cybersecurity.

This *Chaillot Paper* – which uses space exploration as a metaphor to demystify some of the concepts and challenges linked to cyber-related policymaking – focuses on the EU's cyber sanctions regime. The newly-established regime represents a significant achievement in the EU's ambition to defend the rules-based international order, and ensure broader global adherence to agreed norms of responsible behaviour in cyberspace. However, the growing complexity of cyber threats and the proliferation of malicious actors in the cyber domain indicate that the scale of the challenges ahead should not be underestimated.

The EU's autonomous cyber sanctions regime constitutes a unique solution to the challenge of compliance with international law and norms of state behaviour. Taking account of the lessons derived from other sanctions regimes adopted by the EU in the past, the volume addresses a number of key issues relevant for ensuring the maximum effectiveness of the new regime. These include the problematic nature of attribution, state responsibility in cyberspace, listing and de-listing criteria, the principle of due diligence or the potential impact of cyber sanctions on the physical world.

EUROPEAN UNION Institute for Security Studies

Publications Office of the European Union

ISBN 978-92-9198-849-5
CATALOGUE NUMBER QN-AA-19-005-EN-C