CHAPTER 3

SPACE EXPLORATION

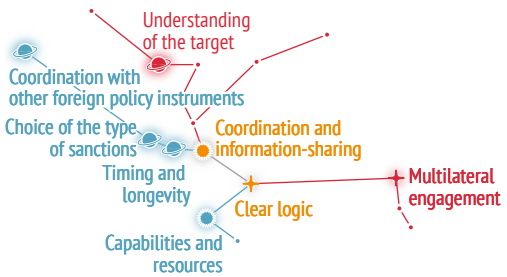
Mapping the EU's cyber sanctions regime

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.

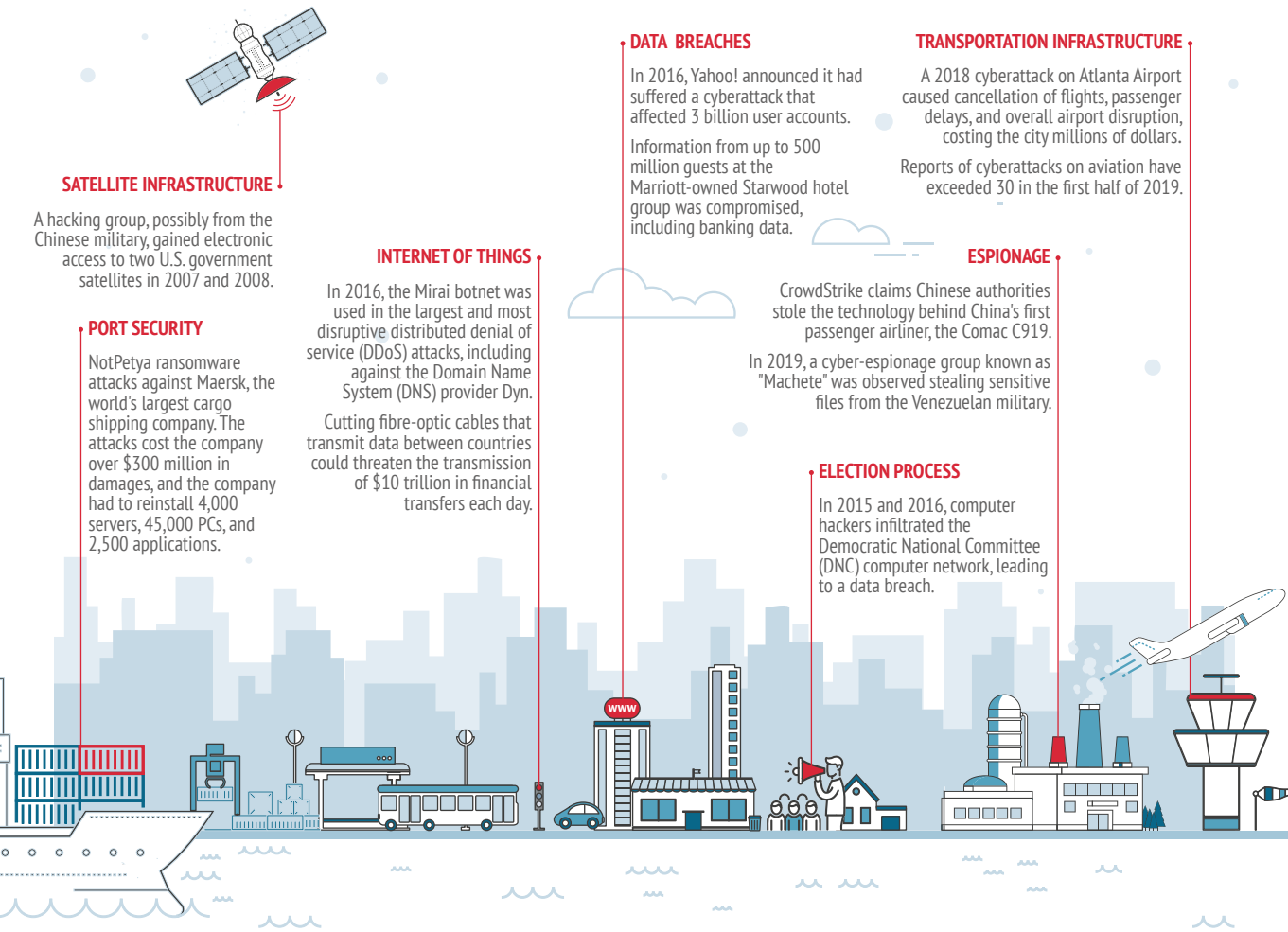
Another question worth considering is that of the link between the level of preparedness and capacities of an individual member state and the potential impact of a cyber operation targeting that member state. It is not difficult to anticipate a situation where a group of EU member states suffer significant 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.