Between Strategic Autonomy and International Norm-setting

The EU's Emergent "Cyber-Sanctions" Regime

Yuliya Miadzvetskaya

Today's world is characterized by an increased strategic competition and rising threats to multilateralism and a rules-based order. In this fast evolving environment, the EU has shifted from its traditional 'values-based' approach in foreign policy to a 'principled pragmatism'. This holds that the European Union should solidify relations with countries with shared values, while also engaging strategically with rivals. The EU's goal is to protect its strategic interests in a world marked by the US-China rivalry, a more uncertain relationship with the US, and Russia's growing ambitions in their shared neighborhood.

The present chapter examines some aspects of the EU's efforts to secure its autonomy in an emergent terrain for international competition: cyberspace. The analysis will begin with an explanation of the broader context for the EU's approach to cybersecurity, which should be understood as part of the Union's longstanding pursuit of 'strategic autonomy' in an increasingly competitive geopolitical environment. It then offers a description of deterrence theory and its application to cyberspace, before turning to the development of the EU 'Cyber Diplomacy' toolbox and targeted restrictive measures in response to cyberattacks. It will then seek to assess the deterrence potential of restrictive measures on the basis of some generic attributes of the concept of deterrence, identified in rich theoretic contributions on deterrence theory and cyberspace. It concludes that while sanctions might appear to be ineffective and non-aligned with the operational characteristics of the cyber domain, their potential for establishing good practices should not be discarded. They should instead be used as a vehicle for promoting and informing the international discourse on the norms of responsible state behavior in cyberspace.

Strategic Autonomy in Cyberspace

EU policymakers increasingly believe that the EU has to take a greater responsibility for its cybersecurity challenges if it wishes to overcome its traditional dependence on the NATO and the US in the military domain. The EU's ability to engage with partners whenever possible and act autonomously whenever necessary will increase the EU's credibility at the international stage.

"Building greater resilience and strategic autonomy" are accordingly listed as EU cybersecurity strategy aims (European Commission 2017: 2). A stronger EU cyber 'actorness' requires the elimination of cyber threats that undermine the EU's strategic independence. The concept of 'strategic autonomy', however, is vaguely defined, and is at times used interchangeably with self-sufficiency or sovereignty (Franke/Varma 2019). Furthermore, all the Member States can project their own understanding into this concept, which makes it even more difficult to establish common definitions.

The term 'strategic autonomy' is thought to have come into the EU discourse from French defense policy circles, where it has long been in use (Timmers 2019). Strategic autonomy is mentioned in a 1994 French white paper on defense (République Francaise 1994). The French president, Emmanuel Macron, is a strong advocate of strategic autonomy and even referred to "Europe's autonomous operating capabilities" in his 2017 Sorbonne speech on the future of the European Union (Macron 2017). Defense cooperation is one of the domains where France could potentially assert European leadership over Germany, in particular with the UK leaving the EU.

Strategic autonomy is often associated with a closer, more efficient security cooperation between member states; one that would enable the EU to take decisions with regard to its own future independently from other global players (Brustlein 2017: 27). It also relates, however, to the EU's economic and cyber resilience, which consists in deciding on its own trade policy and reinforcing its digital sovereignty. For these purposes, the European Council has recently invited the Commission to identify and decrease economic dependencies on external actors by diversifying production and supply chains as well as fostering production and investment in Europe (2020a). However, not all the EU Member States share the same enthusiasm for the catchphrase of 'strategic autonomy'; some view this initiative as a "protectionism in disguise" (Tamma 2017).

The EU has undertaken several initiatives for fostering its strategic autonomy and increasing its competitiveness in the cyber domain. They can be divided into three main areas: resilience, defense and deterrence building in cyberspace. These are the three core elements of the EU 2017 cybersecurity strategy.

Resilience encompasses "the capacity to withstand, recover from, and adapt to external shocks" (Dupont 2019: 2). It implies the establishment of solid structures capable of responding to cyber-attacks in the Member States and at the EU's institutional level. In this regard, the European Union Agency for Cybersecurity (ENISA) plays a crucial role in fostering EU cyber resilience and supports the implementation of the Directive on security of network and information systems (European Parliament and Council 2016). In addition, an EU cybersecurity certification framework was set up by the Cybersecurity Act (European Parliament and Council 2019) to strengthen resilience of ICT products and services.

When it comes to defense, the European Defense Fund (EDF) was established in 2017 to support cooperation between Member States, industry, research centers, and universities. The Coordinated Annual Review on Defense (CARD) has been operating on a trial basis since 2017. It monitors the defense plans of member states in order to ensure a greater coherence in defense spending (van Reybroeck 2019). In 2017, the decision was adopted to establish the Permanent Structured Cooperation on security and defense (PESCO), as laid down in Articles 42(6) and 46 of the Treaty on the EU (TEU).

Aspects of economic policymaking have also been linked to the strategic autonomy agenda. Concerned about investments in European high-tech and infrastructure, the EU rolled out a regulation for the screening of foreign direct investments on the grounds of security or public order in 2019. Here, the EU followed the US lead on the protection of sensitive domains from foreign control. The US introduced oversight over foreign investments via the 2018 Foreign Investment Risk Review Modernization Act (FIRRMA). This legal framework controls key US technologies, such as semiconductors, telecommunications, robotics and AI (Zable 2020).

Alongside these new initiatives in the fields of defense and foreign policy, the EU has also sought to establish elements of 'strategic autonomy' in the cyber domain. Over the past decade, widespread cyberattacks, remote controlled weaponry and the hyped concept of 'cyberwars' and 'cyberwarfare' posed a need for strategies to deter their use. Deterrence has long been a part of mainstream foreign policy discussions. But it is now applied in the cyber domain, as prominently as it is on land and in the air, sea and space. While the EU is just in the beginning of establishing its cyber deterrence strategies, the US, benefitting from a less fragmented decision-making and better cyber capabilities, was already more effective in applying sanctions or criminal charges against government-sponsored hackers (Department of Justice 2018a). For instance, in 2016, the US imposed sanctions against nine Russian parties, including two Russian Federal Security Services, the Main Intelligence Directorate (GRU) and Federal Security Service (FSB), over their alleged elections interference (White House 2016a). A North Korean programmer was accused by the US Department of Justice of involvement in several cyber-operations, including the WannaCry attack (White House 2016b). In October 2018, the US charged seven Russian GRU officers with compromising computer networks used by various sporting and anti-doping organizations, a US nuclear power company, the Netherlands-based Organization for the Prohibition of Chemical Weapons (OPCW) and the Switzerland-based Spiez laboratory (Department of Justice 2018b). In July 2020 the US announced an indictment against Chinese nationals for computer intrusion campaigns (Soesanto 2020). The US "cyber sanctions" program was in place for five years. Several Russian, Iranian and North Korean entities were put on the US Department of the Treasury's Office of Foreign Assets Control (OFAC) "cyber sanctions" list.

Deterrence also made its way into the EU discourse, with the EU's acknowledgement of the threats that cyberattacks pose to critical infrastructures, democratic processes and international stability. The EU uses alternative non-military instruments of deterrence and coercion so as to position itself as a force for peace. Deterrence is mentioned in the 2017 Communication "Resilience, Deterrence and Defense: Building strong cybersecurity for the EU" and constitutes one of the cornerstones of the EU cybersecurity policy (European Commission 2017). Deterrence is crucial for addressing new cybersecurity risks and discouraging potential perpetrators. The latter is done by the use of (or the threat of the use of) criminal and political measures in response to cyberattacks. In contrast to individual Member States, the EU's greater reach as a bloc allows it to influence the cost-benefit calculus of malicious actors and thus contribute to the maintenance of the status quo.

The EU deterrence toolbox was recently expanded with several instruments of influence, including sanctions and traditional 'name and shame' practices. The US was the first country to add sanctions to its existing deterrent tools (White House 2015). Following the US example, the EU introduced a legal framework in May 2019, which provides for restrictive measures in response to cyberattacks. Incorporating sanctions as a deterrence measure is intended to strengthen the EU's capacity to respond to malicious cyber enabled activities, which undermine its economic, political and security interests (European Commission 2017). This framework also strengthens the EU's position internationally since it allows it to signal an unacceptable behavior in cyberspace.

At the end of July 2020, the EU imposed its first 'cyber sanctions'. The EU emulated to a large extent the US sanctions and listed Russian, Chinese, and North Korean entities and individuals which have already been sanctioned by the US (European Council 2020b). The symmetry between the EU and US sanctions signifies both sides' readiness to act as a bloc on cybersecurity issues in order to have a stronger position in the big power competition to set a framework of responsible state behavior in cyberspace and sanction destructive, disruptive and destabilizing cyber-activities.

Deterrence in Cyberspace

Deterrence is identified as one of the main strategies for preventing cyberattacks. It can be understood as a form of coercion entailing a manipulation of an adversary's estimation of the cost-benefit calculation. Deterrence also refers to the use of a threat "explicit or not" by one party, with the objective of persuading another party to change behavior or maintain the status quo (Quackenbush 2011: 741). The concept of mutually assured destruction, which creates the looming threat of mutual annihilation in the case of one party launching an attack on another, represents maybe the most famous example of nuclear deterrence (Crosston 2011).

Deterrence has become a widely used concept in cybersecurity discourse. The term "(cyber)deterrence" was coined by Professor James Derian in a 1994 issue of *Wired Magazine*, which examined the potential deterrent effect of network technologies on the physical environment. Many scholars agreed that the conventional concept of deterrence, as applied to the kinetic environment, is difficult to transpose to the unique nature of cyberspace for a wide range of reasons (Libicki 2009: 3). Libicki (ibid: 40-41) laid out some major elements that would differentiate (cyber)deterrence from nuclear deterrence. First, the logic of deterrence in cyberspace is undermined by the difficulty of ascribing responsibility for attacks (on which more below). Secondly, it is difficult to clearly communicate the threshold of an action leading to a reprisal (Libicki 2017). It is one thing to assess an attack that blows up a refinery; it is another to assess a cyberattack that damages the refinery control system (Libicki 2009: 52). Furthermore, it is not clear what the threshold of response should be and how further escalation can be avoided (ibid.).

Critics of the application of deterrence theory in the cyber realm argue that there are "fundamental inconsistencies between the theory and the nature of cyber conflicts and cyberspace" (Taddeo 2018: 340). While some scholars insist on the need to reformulate and extend classic deterrence thinking to the cyber domain (Nye 2017) others call for a sharp break from the deterrence-centric paradigm (Harknett/Nye 2017). For instance, Fischerkeller and Harknett (2017) criticized deterrence for its strategic inertia in creating behavioral effects, which exacerbates, in their opinion, the absence of US leadership in shaping the parameters of acceptable behavior in cyberspace. They propose, instead, to replace a strategy of operational restraint and reaction with persistent engagement in advancing US interests. In other words, this would mean a shift from threat-based approach to capabilities-based strategy; from what threatens the US to what the US can do to proactively shape cyberspace. In 2018 the US Cyber Command and the National Security Agency (NSA) announced a strategy based on "persistent engagement" and "defend forward" (The Economist 2020). This can be understood as a return to pre-emption: not so much 'striking back' as 'striking first'.

Across this literature, denial and retaliation are commonly identified as two types of deterrence strategies. Denial is the defensive aspect of deterrence, whereas punishment is the offensive one. Deterrence by denial focuses on preventing an attack from occurring and denying an enemy an ability to cause damage. In contrast, deterrence by retaliation implies the threat of coercive measures to change behavior (Taddeo 2018). Cyber-sanctions offer a 'third way' of shaping cyberspace between passive deterrence and a US-style 'striking first' approach. The deterrent potential of cyber-sanctions could be leveraged as a means of regulating cyberspace and setting norms of responsible state behavior in cyberspace.

Deterrence by denial is difficult in cyberspace, since many vulnerabilities are not known until they are exploited by malicious actors. Sometimes knowledge of vulnerabilities is kept secret as a form of bargaining. As Thomas Schelling has observed, "the power to hurt is most successful when held in reserve" (2008: 3). Furthermore, potential perpetrators are many and diffuse. Consequently, no system in the world would be fully defended against infiltration attempts. What counts in this context is the resilience of the system and its "capacity to withstand, recover from, and adapt to external shocks"

(Dupont 2019: 2). 'Deterrence by denial' in the US discourse echoes 'resilience' in EU official documents. Resilience, as described in the EU 2013 Cybersecurity Strategy (European Commission 2013), aims at strengthening prevention and early warning mechanisms with regard to cyberattacks. This is deemed crucial for the maintenance of a well-functioning internal market.

As an illustration, Estonia represents one of the most prominent examples of deterrence by denial. After being targeted by the first (allegedly) State-sponsored distributed denial-of-service (DDoS) attack, Estonia launched an initiative called the "Data Embassy", with the objective of backing-up data storage facilities outside its borders (Sierzputowski 2019: 227; see also Myatt in this volume). In 2017 an Estonian data embassy was finally established in Luxembourg in order to ensure national digital continuity and service functionality "no matter what" (ibid.). 'Physical' embassies enjoy a wide range of immunities under the Vienna Convention on diplomatic relations. Estonia is setting the tone by bringing the same concept to the cyber world.

The key elements of deterrence theory were described by Morgan (2003: 8). They involve the assumption of a conflict, the assumption of rationality, the concept of a retaliatory threat, the concept of unacceptable damage, the notion of credibility, and the notion of deterrence stability. Taddeo discusses how ineffective those elements are when applied to a (cyber)conflict (2018: 340). She does so by suggesting the minimalist model of international deterrence (DM) defined according to the deterrence theory. The minimalist model of international deterrence (DM) includes three core elements: the attribution of responsibility for attack, deterrence strategies, and the capability of the defender to signal credible threats to potential attackers (Taddeo 2018: 340). For the purposes of this study, we will assess how sanctions in response to cyberattacks fit into the logic of deterrence by combining the elements of the Minimalist model of international deterrence and the deterrence attributes identified by Morgan (2003). The next section will provide an analysis of the development of a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities or the "EU Cyber Diplomacy Toolbox". Particular attention will be paid to restrictive measures as a deterrence instrument of the EU Cyber Diplomacy.

Restrictive Measures as a Deterrence Instrument in EU Cyber Diplomacy

The EU sanctions regime is designed to strengthen the EU's leadership in setting up a set of rules for regulating cyberspace. The efficiency and challenges of restrictive measures[1] from political, human rights and attribution perspectives have been examined elsewhere. This work will not repeat them but will instead explore restrictive measures as a concrete practical example of (cyber)deterrence tools available to the EU.

The EU's development of collective responses to cyberattacks has rested on a recognition that the multiplication of cyberattacks and their destructive character required a different response, beyond the conventional defense of networks and resilience-building paradigm. For the first time, the possibility of a joint EU diplomatic response to cyberattacks was mentioned in the Council conclusions on Cyber Diplomacy in February 2015 (European Council 2015). In 2016, the Dutch Presidency submitted a 'non-paper'[2] on "Developing a joint EU diplomatic response against coercive cyber operation", which argues that cyber diplomacy is one of the tools to influence a rational cost-benefit analysis of State and non-State actors by increasing the costs of coercive cyber operations and establishing a deterrent effect (European Presidency 2016).

While the resilience and security of networks are essential for preventing and mitigating the consequences of cyber operations, a broader response and a comprehensive use of a multitude of policy instruments were held to be required. The use of cyber diplomacy tools was identified as an appropriate means to deter state and non-state actors from carrying out cyberattacks for politico-military purposes. A common and comprehensive approach to cyber diplomacy can also contribute to the "mitigation of cybersecurity threats, conflict prevention and greater stability in international relations through the use of diplomatic and legal instruments" (European Council 2015).

The Council confirmed the added value of the Joint EU Diplomatic Response to Malicious Cyber Activities in the conclusions of June 2017. These conclusions endorsed that the EU must clearly signal the likely consequences of an EU response to cyber operations so as to influence the behavior of potential aggressors (European Council 2017a). In October 2017, the Council put for-

[1] Sanctions and restrictive measures will be used interchangeably in this chapter. Restrictive measures refer to asset freezes and visa bans with regard to listed individuals.

[2] Informal document issued to facilitate negotiations.

ward the implementing guidelines for the Framework development (2017b). The measures presented therein refer to a range of diplomatic actions to be undertaken by the EU and Member States. They include preventive, cooperative and stability measures, EU support to Member States' lawful responses, and restrictive measures within the CFSP. The above-mentioned measures could be used "either independently, sequentially or in parallel" as part of a comprehensive EU approach (ibid.).

Preventive measures encompass EU-supported 'Confidence Building Measures', including initiatives in third countries through the European Neighbourhood Instrument (ENI) or any other relevant financing instruments. They also include awareness-raising on EU policies, such as EU-led political and thematic dialogues, particularly cyber or security dialogues. Cooperative measures refer to EU-led political and thematic dialogues or EU-diplomatic *démarches* to facilitate the peaceful resolution of an ongoing incident. Stability measures are understood as statements expressing concern or condemning general cyber trends on behalf of the EU, for instance statements by High Representative of the EU; EU Council Conclusions or démarches by the EU delegations as a way to signal the likely consequences of a malicious cyber activity.

Possible EU support to Member States' lawful responses refer to non-forcible and proportionate countermeasures to compel or convince an attacker to change their behavior. In grave instances, cyberattacks could amount to a use of force or an armed attack within the meaning of Article 51 of the Charter of the United Nations. In this case, Article 42(7) TEU (the "Defense Clause") may be invoked by an attacked Member State to ask the EU for aid and assistance.

Restrictive measures, in turn, are usually meant to bring about a change in behavior and can include, *inter alia*, travel bans and the freezing of funds or economic resources. Sanctions of this nature constitute a central instrument of the EU Common Foreign and Security Policy (CFSP). Restrictive measures have as their objective the maintenance and restoration of international peace and security, the fight against terrorism and the proliferation of weapons of mass destruction, the upholding of respect for human rights, democracy and the rule of law. The EU is the second most active user of restrictive measures, surpassed only by the US (Russell 2018).

Sanctions have an inherently preventive character and are not necessarily adopted in response to a breach of an international obligation (Ruys 2016). For instance, the UN Security Council does not need to establish a violation of international law for their enactment, but must find a "threat to the peace, a breach of the peace or an act of aggression" in the meaning of Article 39 UN Charter (Kelsen 1948: 789). Generally, sanctions pursue three purposes, namely:

a) to coerce or change behavior
b) to constrain access to resources needed to engage in proscribed activities, or
c) to signal and stigmatize (van den Herik 2014: 433).

In June 2017, the European Council identified restrictive measures as a suitable foreign policy instrument in order to mitigate cyber threats and change the behavior of aggressors in the long term (2017a: 5). Since sanctions represent a traditionally contentious topic, discussions of the EU's capacity to deter cyberattacks through political measures were slow moving. The European Council (2018a) stressed the need to move forward in the work on attribution of cyberattacks and the practical use of the cyber diplomacy toolbox in its conclusions of June 2018. In October of the same year, the European Council (2018b) endorsed the objective to strengthen EU resilience against cyber-attacks and to conclude negotiations on all cybersecurity proposals before the end of the legislature. However, work was progressing slowly since many questions remained as to how the sanctions should be deployed and whether they would work at all.

The 2019 European Parliament elections, deemed 'Europe's most hackable', hastened the adoption of the new "cyber sanctions" framework, which came into being on the 17th of May—just a couple of days before EU citizens headed to polls. The new sanctions regime was introduced based on the traditional two-step approach. First the CFSP decision, which sets out the overall sanctions framework, is adopted by the Council on the basis of Article 29 TEU. Then the CFSP decision is implemented by the accompanying regulation on the basis of Article 215 TFEU.

When viewed from the perspective of international law, sanctions, if defined by the objective of a measure, can possibly amount to retorsion measures. Retorsion measures are measures of unfriendliness vis-à-vis another state but are intrinsically legal (Ruys 2016). They do not necessarily constitute a response to an internationally wrongful act, contrary to countermeasures, which are taken in response to a violation of an international obligation. Countermeasures are law enforcement measures meant to induce a

State to comply with its obligations. They are not punitive; they are by nature temporary and limited to a non-performance of an international obligation.

Sanctions, mentioned in the Cyber Diplomacy Toolbox, are targeted measures and they do not lead to the attribution of responsibility to a State. Nevertheless, Member States are free to make their own determinations with respect to the attribution of cyberattacks. It is thus incorrect to compare targeted sanctions under the EU's restrictive measures to either retorsion measures or countermeasures. First of all, both retorsion measures and countermeasures are taken in inter-state relationships, whereas the EU "cyber sanctions" framework applies to non-State actors and does not entail an attribution of State responsibility. Secondly, countermeasures constitute a response to a prior internationally wrongful act, which is not true for EU sanctions in response to cyberattacks. Thirdly, it is not established yet whether a cyber-operation amounts to a violation of an international legal obligation and, thus, triggers a state responsibility, as suggested by the authors of Tallinn Manual in Rule 14 (Schmitt 2017).[3] Fourthly, there is no general consensus on the application of countermeasures in cyberspace. The international legal framework was not designed to accommodate violations caused by cyberattacks; and persistent attempt to apply international law to cyber threats is sometimes compared to fitting square pegs into round holes (Anderson 2016: 141).

Restrictive Measures as a (Cyber)deterrence Instrument

How effective, then, are restrictive measures as a response to cyberattacks? The present section will assess the deterrence potential of restrictive measures on the basis of some generic attributes of the deterrence identified in rich theoretic contributions by Morgan (2003) and Taddeo (2018). First, we will analyze what constitutes a conflict in cyberspace from the deterrence perspective and what type of threat triggers the activation of the EU "cyber sanctions" framework. Secondly, we will explore the limits of the assumption of rationality when applied to restrictive measures in response to malicious cyber activities. Thirdly, we will analyze the EU's potential for making a deterrent

[3] According to Rule 14: "A State bears international responsibility for a cyber-related act that is attributable to the State and that constitutes a breach of an international legal obligation."

declaration and signal clear consequences to potential attackers through recourse to restrictive measures.

The Assumption of a Conflict

The assumption of a conflict constitutes one of the main elements of deterrence. Accordingly, the nature and intensity of a conflict will have a significant impact on the deterrence strategy. No one questions the destructive potential of cyberattacks. As an illustration, Michael Hayden, the former Central Intelligence Agency (CIA) and National Security Agency (NSA) director, compared the computer virus StuxNet to a new weapon (Greenberg 2017). According to Estonia's ex-president Toomas Hendrik Ilves, there is no need for missiles to destroy the infrastructure of a rival state, since everything can be orchestrated online (Sierzputowski 2019: 226). To some extent, this cyberwar scenario partly materialized in Ukraine in 2015, when an unprecedented hack of Ukraine's electricity grid caused an electricity blackout. The WannaCry and NotPetya attacks similarly demonstrated the extent of the damage to people and infrastructure that malicious cyber-enabled operations can inflict.

As per the 2019 European Council Decision on cyber sanctions, restrictive measures can be taken in response to performed and attempted cyberattacks of a "significant effect". It seems, however, disproportionate for the Council to suggest the use of sanctions as a response to an attempted, but deterred attack with a potentially significant effect. It is also unclear what the yardstick is for measuring the significance of an attempted attack. Uncertainty is particularly dangerous in a situation where damage prediction is crucial for successful deterrence and compliance with the principle of proportionality. The Council decision provides a list of criteria relevant for the assessment of an attack's impact. Among them, it mentions "the scope, scale, impact or severity of disruption caused" (2019). To perform such an assessment, an important cooperation effort on behalf of Member States will be required. Furthermore, the Council mentions as relevant assessment criteria "the number of natural or legal persons, entities or bodies" affected by a cyber-attack as well as "the amount of economic loss and the amount or nature of data stolen" (ibid.). Measuring the impact of a cross-border cyber-incident is a complex task. There is a traditional reluctance to share data concerning the destructive effect of cyber operations on economic and societal activities, essential services, critical state functions and public order or public safety. More guidance is required with regard to the calculus applied. Will it require setting up

https://doi.org/10.14361/9783839457474-011 https://www.inlibra.com/de/agb - Open Access -

a specialized body empowered to perform such assessment? Or will it be performed by the EU Intelligence Analysis Centre (INTCEN)[4] or the Horizontal Working Party (HWP) on Cyber Issues within the Council of the EU?

The activation of the adopted framework is foreseen in response to a cyberattack which constitutes an 'external threat' not only to the Union or its Member States, but also to third States or international organizations. The Council provides several illustrations of cyberattacks which constitute external threats. Such attacks entail damage to critical infrastructures or services—such as energy or transport; or the disturbance of critical State functions, such as the storage or processing of classified information. The notion of 'threat' is difficult to square with the existing terminology. It is unclear what threshold of an attack the Council refers to. Three interrelated thresholds are applied in international law and include: the threat or use of force; armed attack; and the threat to peace, breach of peace, and act of aggression (Delerue 2020: 276). In the EU Treaties, the reference to "threat" is made on two occasions. First, it is made in the context of "Solidarity Clause" (Art. 222(1)(a) and (4) TFEU), which conventionally refers to terrorist attacks. Pursuant to "Solidarity Clause", the European Council shall ensure the regular assessment of the threats facing the Union. The second reference to a "threat" is made under Article 347 TFEU, which provides for cooperation between Member States in order to alleviate the disturbing impact of measures taken in the event of a serious international tension constituting a threat of war.

It is not surprising that the EU does not try to align its vocabulary with the existing international legal framework. Instead, the Council introduces a new concept of "an external threat". This "escapism" from the international legal framework can be interpreted in a number of ways. First, while the EU accepts the application of international law in cyberspace, it has still not unveiled its views as to the interpretation of international legal rules. Second, the EU is traditionally known for its effort to preserve the autonomy of its legal order. Govaere (2018) compares the EU legal order to the autonomous EU balloon, which needs to be shielded from puncturing by international law interference. Thirdly, American exceptionalism or "New Sovereigntism", which has fuelled US foreign policy in recent years, has undermined transatlantic trust and the value of international law commitments (Spiro 2004). Some recent examples of the resistance of the US to the force of international law include the decision to leave the World Health Organization (WHO), and the

[4] INTCEN is a network of security services of Member States.

https://doi.org/10.14361/9783839457474-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY

Open Skies Treaties, alongside its withdrawal from the 1987 Intermediate-Range Nuclear Forces (INF) Treaty between the United States and Russia and from the Iran nuclear agreement.

We should also note the emphasis the European Council puts on the external origin of a cyberattack. This is defined on multiple levels:

a) the attack(s) are carried out from outside the Union;
b) the attack(s) use infrastructure outside the Union;
c) the attack(s) are carried out by any natural or legal person, entity or body established or operating outside the Union; or
d) are carried out with the support, at the direction or under the control of any natural or legal person, entity or body operating outside the Union.

The reliance on an external element seems unfit for the operational characteristics of cyberspace. It is technically possible to escape the qualification as "external". Different deception techniques via 'spoofing' and 'false flags' may be displayed in order to pretend that an attack originates within the EU territory. Establishing a link between a perpetrator and any natural or legal person, entity or body supporting, directing or controlling the performance of the operation in question is a difficult matter.

The Assumption of Rationality

Deterrence aims to convince another actor not to attack by threatening unacceptable damage; or by altering their calculations with respect to risks, response and reward (Nye 2017: 45). Rationality is therefore intrinsic to deterrence theory building. It entails forecasting the impact of expectations about benefits and costs on the adversary's behavior. However, the conventional assumption of rationality is usually ineffective in cyberspace. Some cyberattacks are opportunistic; the perpetrators are diffuse; and the costs of engaging in malicious cyber activities are often limited.

The EU Cyber Diplomacy Toolbox presumes a rational challenger as well. Restrictive measures are adopted with the objective of influencing the behavior of potential aggressors over the long term. The type of measures chosen by the EU points out to their mostly economic character: travel bans and the freezing of funds and other economic resources of natural or legal persons, entities or bodies that are responsible for (attempted) cyber-attacks. To constitute an efficient deterrent tool, the measure should be able to influence a cost-benefit analysis of perpetrator. The deterrent effect of sanctions would currently be meaningless where a perpetrator did not have any economic resources in the territory of the EU. EU restrictive measures, in contrast to American secondary sanctions, do not have an extraterritorial reach and apply to EU-based entities solely. Against this background, one could claim that the EU should not keep its expectations too high with regard to the dissuasive effect of its sanctions.

As follows from the implementation guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities (2017b: 4), restrictive measures in response to cyberattacks must conform to the principle of utility in a sense that they need to be "proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact" of an aggressive behavior in cyberspace. In general, sanctions are not punitive measures and have a preventive character. This view was confirmed by the European Court of Justice (ECJ) in the seminal Kadi II judgement (ECJ 2013: §130). In a similar vein, the International Law Commission (ILC) rejects the idea of "punitive damages" (ILC 2001). It stresses that countermeasures must be proportionate to the original wrongful act(s), temporary, and should be aimed at inducing the State to comply with the law. The principle of proportionality is also enshrined in Article 51 of the Articles on State responsibility. The ICJ expressed in the Gabčíkovo-Nagymaros case with respect to the proportionality requirement that the effects of a countermeasure must be commensurate with the injury suffered (ICJ 1997: §85). The authors of Tallinn Manual codified this in Rule 23, which reads as follows: "Countermeasures, whether cyber in nature or not, must be proportionate to the injury to which they respond" (Schmitt 2017).

It follows that a restrictive measure shall be adjusted to the damage suffered. However, determining the impact, value and type of damage of a cyberattack is not an easy exercise. It can be a serious hurdle to guarantee that a restrictive measure is proportionate to a performed cyber-operation. Estimation failures are dangerous and can trigger further escalation. Furthermore, restrictive measures, when targeted, are limited as to the number of options available. They entail either travel bans or the freezing of funds. There is not much flexibility for the EU as to the selection of scalable deterrence tools.

Deterrent Declaration and Credibility

Signaling credible threats is one of the elements of the minimalist model of international deterrence suggested by Taddeo (2018). It refers to the capacity of deterring an attacker through the prospective (signaled) threat of coercive measures. Deploying an appropriate deterrence strategy and clearly conveying a coercive message is crucial for an effective retaliation. There should be a clear understanding of what is acceptable and what are red lines.

Efficient deterrent declaration presupposes a number of elements. The deterrent declaration must be loud and clear so the target cannot misread it; it should be clearly mentioned in national policy, and be consistently echoed in the words and actions. For instance, NATO has already declared that a cyberattack could lead the alliance to invoke its Article 5 collective defense clause. This Statement aims to have a deterrent effect. Implicit or explicit threats of restrictive measures constitute another example of deterrent declarations.

The deterrent effect of the EU framework on restrictive measures is weakened by complexities of attribution and by political divisions within the EU. The ambiguities of cyberspace do not simply reflect the traditional challenges that are present in other domains, but are particularly exacerbated by operational features of the cyber realm (Roscini 2015). As it has been noticed "the Internet is one big masquerade ball" where the possibility of spoofing and masking IP addresses makes more difficult the identification of a computer or computers used to carry out a cyber-operation (Roscini 2015: 234). Contrary to the Cold War bipolar world, today's cyberspace is characterized by the unprecedented rise of active and sophisticated non-state actors. Since much ink has been spilled debating the contentious issue of political, legal and technical attribution, this contribution will limit itself to reaffirming the persistence of human-machine gap and of the challenge of establishing a sufficient legal nexus between non-state actors and a non-EU state.

Moreover, the EU often does not have one common stance on the issue of attribution. Unlike a few member states, which have publicly attributed cyberattacks, the EU has not taken any act of attribution or follow-up with regard to potential perpetrators. The question of collective attribution of cyber-attacks by the EU was passed over in silence on multiple occasions. While the UK and Denmark attributed the NotPetya cyberattack to the GRU (Russian Military Intelligence) and some Member States issued statements of support, the April 2018 Council conclusions were limited to a formal "condemnation of the malicious use of information and communications technologies (ICTs)"

(European Council 2018c). The same discrepancies became obvious at the institutional and governmental levels with respect to the attacks on the offices of the Organisation for the Prohibition of Chemical Weapons (OPCW) in The Hague.

The Decision of the European Council (2019) on cyber sanctions highlights that targeted sanctions should not be viewed as the attribution of responsibility to a state. Nevertheless, this delimitation between individual perpetrators and states remains rather artificial. The practice shows that a majority of cyberattacks with substantial consequences, such as StuxNet, WannaCry and NotPetya, were orchestrated at the request and with the support of governments.

The credibility of EU cyber sanctions is currently being tested by cyberattacks on Georgia and the German Parliament. In October 2019, Georgia was targeted with a number of cyberattacks undermining the websites and servers of several governmental agencies, including that of the President of Georgia, courts of Georgia, NGOs, local governments and various organizations. In February 2020, the Georgian Foreign Ministry Stated that the Russian General Staff Main Intelligence Directorate (GRU) carried out a "widespread, disruptive cyber-attack" (Agenda.ge 2020). The EU along with its Member States condemned the cyberattack and reaffirmed its willingness to continue to assist Georgia in increasing its cyber resilience (EU High Representative, 2020). In contrast to some Member States (Netherlands, Latvia, UK) and other partners (US, New Zealand), the EU did not attribute this cyberattack to Russia. Some commenters (Nakashidze 2020) were wrong in assuming that the general statement of condemnation constituted an act of attribution. The EU's reaction to a cyberattack on Georgia was passive despite the fact that the EU has the possibility of applying restrictive measures even in response to a cyberattack on a third country, pursuant to Article 1(5) of the Council Decision (2019). In the case of Georgia this could be justified by its special status as an associated partner. Georgia and the EU have an ambitious Association Agreement in place, which has as an objective the full integration of Georgia into the EU single market.

The cyberattack on German Parliament was another test of the deterrent effect of the 'cyber-sanctions'. In the present case, the perpetrator is known; and Germany considered triggering the framework. As this chapter was being written, the EU imposed sanctions against two Russian military intelligence officers and "military unit 26165", also known as "APT28", "Fancy Bear", and believed to be behind the breach of the German *Bundestag* in 2015 (European Council 2020c).

The Role of Restrictive Measures in Shaping Responsible State Behavior

While they may seem ineffective at first glance, restrictive measures nonetheless have a significant signaling potential. It will be argued in this section that they can serve as an instrument for cultivating a culture of compliance and responsibility in the cyber domain. This is in line with the European Union's objectives as outlined in the Lisbon Treaty, which expressly states in Article 3(5) that the Union "shall contribute to […] the development of international law, including respect for the principles of the United Nations Charter". In addition, Article 21 of the Treaty commits the EU's action at the international scene should aim at safeguarding its security, consolidating principles of international law, strengthening international security, and promoting an international system based on stronger multilateral cooperation and good global governance. The EU also committed to strongly "uphold that existing international law is applicable to cyberspace" (European Council 2019). Sanctions have an important role to play in framing a normative framework by targeting, signaling and deterring a state's behavior when it crosses red lines.

Respect for international law and norms of responsible state behavior legitimize the actions of a state as a good global actor. Nevertheless, the questions remain as to the adequacy of the existing international legal framework when applied to cyberspace. Whereas some states, including Russia, favor the negotiation of new legal norms others led by the US find the existing legal norms sufficient (Korzak 2015).

In the seminal 2013 report of the UNGGE (United Nations Group of Governmental Experts on Information Security), participating states agreed that international law regulates the cyber domain and forms one of the key pillars of stability in cyberspace. However, there is no common understanding of how international law should apply in cyberspace. The problem is compounded by a persistent general disagreement over the potential use of the right to self-defense and the law of armed conflicts in cyberspace (Delerue 2019: 297). In the 2016-2017 discussions over a new report of the UNGGE, Russia and Cuba opposed equating the malicious use of ICTs to the concept of "armed conflict" under Article 51 of the UN Charter. Remaining divergences in views on international norms caused the failure of the 2017 UNGGE to concur on a final report.

In 2018, two separate processes were established under the auspices of the UN. Russia sponsored the resolution, which provided for the establishment of an Open-Ended Working Group (OEWG) open to any UN Member. The other resolution under the leadership of the US provided for a new Group of Governmental Experts (GGE) with a smaller membership. While Russia and the US presented the two resolutions as mutually exclusive, many countries voted for both of them (Delerue 2020: 210). Embarking in two overlapping discussions is a difficult endeavour, likely to aggravate the present lack of consensus.

Since it is not clear what international legal rules apply to cyber-operations, attribution in this context is reduced to a purely political condemnation without pointing to a specific legal obligation, let alone legal consequences for a wrongful act. A decision to attribute a cyber-operation to another state is often linked to broader policy objectives and is dependent on concrete instruments available in response to such malicious activities. Finnemore and Hollis (2020) explore the implications of cybersecurity accusations, which include three elements: attribution, exposure and condemnation. As a reminder, in accordance with Articles on State Responsibility, the state is responsible for the conduct of its organs, persons or entities exercising elements of governmental authority or those who act under its instructions, directions or control. The principle of due diligence can also serve for the establishment of indirect responsibility in the cyber realm (Chircop 2018, Buchan 2016). Cybersecurity accusations can be made with the objective of deterrence, aid, defense, and contribution to the emergence of new norms and international law (Finnemore/Hollis 2020).

Recent attributions of cyberattacks against Georgia were striking for their omission of an allegedly breached rule of international law. The omission of reference to rules of international law stems from a disagreement as to whether a breach of sovereignty constitutes a rule, which triggers state responsibility or just a principle of international law (Roguski 2020). One can also observe 'gray' area status of cyberattacks, which fall below the threshold of an armed attack, use of force or an internationally wrongful act.

Are restrictive measures capable of filling in the void? Can sanctions compensate the vacuum stemming from the as-yet unclear international legal framework? Would deterrence via sanctions be an efficient way of promoting and clarifying the norms of responsible state behavior? These questions cannot yet be answered, but they are worth reflecting upon. Even more so, for

https://doi.org/10.14361/9783839457474-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY

the EU, which is fundamentally committed to the development of international law. When conventional discussions reach a deadlock, someone needs to think outside the box. Restrictive measures constitute a tool which allow exposure and help to establish the bar for the assessment of what is acceptable in cyberspace. Only through signaling and communicating can the international community succeed in establishing the rules for cyberspace, whether through the codification of customary international law or through a treaty. Against this backdrop, sanctions represent a valuable tool to shape and promote responsible state behavior, even in the absence of a consensus on the interpretation of rules of international law in cyberspace.

Conclusions

The EU is committed to a rules-based international order. This commitment translates into an aspiration to shape, transform and adapt the existing system to a new cyber domain. EU cyber-sanctions, despite their limited strategic effectiveness, could serve as an instrument for cultivating a culture of compliance and responsibility in the cyber domain. Sanctions have an important role to play in framing a normative framework by targeting, signaling and deterring a state's behavior when this crosses red lines. Thus, EU sanctions could help to jump-start a necessary progress of agreeing international law frameworks for cyberspace that is currently stalled at the UN level.

EU cyber-sanctions are designed as deterrence measures for strengthening the EU's leadership in setting up a set of rules for regulating cyberspace. Along with the US, the EU emerges as a significant global actor establishing standards for itself and aligning approaches with other strategic partners. In this context, cyber deterrence via sanctions regime offers a norm-setting a 'third way' between passive deterrence and US-style 'striking first' approach in cyberspace. The development of the cyber diplomacy toolbox is indispensable for the EU if it wants to learn "the language of power" in the competitive cyber domain (Kribbe 2020).

References

Agenda.ge (2020): "Georgia accuses Russia of widespread cyberattack", Agenda.ge, February 20 (https://agenda.ge/en/news/2020/535).

Anderson, T. (2016): "Fitting a Virtual Peg into a Round Hole: Cyber Reprisals." In: Arizona Journal of International & Comparative Law 34/1, pp. 136-157.

Brustlein C. (2017): "Entry Operations and the Future of Strategic Autonomy." In: Focus Stratégique N° 70 bis, p. 27.

Buchan, R. (2016): "Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm." In: Journal of Conflict and Security Law 21/3, pp. 429-453.

Chircop, L. (2018): "A Due Diligence Standard of Attribution in Cyberspace." In: International and Comparative Law Quarterly 63/3, pp. 643-668.

Crosston, M. D. (2011): "World Gone Cyber MAD: How 'Mutually Assured Debilitation' Is the Best Hope for Cyber Deterrence." In: Strategic Studies Quarterly 5/1, pp. 100-116.

Delerue, F. (2019): "International Cooperation on the International Law Applicable to Cyber Operations." In: European Foreign Affairs Review 24/2, pp. 203-216.

Delerue, F. (2020): Cyber Operations and International Law, Cambridge: Cambridge University Press.

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

Department of Justice (2018b): "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations", The United States Department of Justice Press Release, October 4 (https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and).

Derian, J. (1994): "Cyberdeterrence", January 9 (https://www.wired.com/1994/09/cyber-deter).

Dupont, B. (2019): "The Cyber-Resilience of Financial Institutions: Significance and Applicability." In: Journal of Cybersecurity 5/1, pp. 1-17.

ECJ (2013): "Cases C-584/10 P, C-593/10 P and C-595/10 P", European Court of Justice, Commission and United Kingdom v Kadi, Judgment of the Court (Grand Chamber).

EUGS (2016): Shared Vision, Common Action: A Stronger Europe, A Global Strategy for the European Union's Foreign and Security Policy, Brussels: European Union.

European Commission (2013): "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", European Commission Joint Communication JOIN/2013/01, Brussels.

European Commission (2017): "Communication 'Resilience, Deterrence and Defense: Building strong cybersecurity for the EU'", European Commission Joint Communication JOIN/2017/0450, Brussels.

European Council (2015): "Conclusions on Cyber Diplomacy", European Council Report 6122/15, Brussels.

European Council (2017a): "Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox')", European Council Report 10474/17, Brussels.

European Council (2017b): "Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities", European Council Report 13007/17, Brussels.

European Council (2018a): "Conclusions", European Council Conclusions June 28 (https://www.consilium.europa.eu/en/press/press-releases/2018/06/29/20180628-euco-conclusions-final).

European Council (2018b): "Conclusions", European Council Conclusions, October 18 (https://www.consilium.europa.eu/en/press/press-releases/2018/10/18/20181018-european-council-conslusions).

European Council (2018c): "Conclusions on malicious cyber activities—approval", European Council Report 7925/18, Brussels.

European Council (2019): "Decision (CFSP) 2019/797 concerning restrictive measures against cyberattacks threatening the Union or its Member States," European Council Decision OJ L 129I, Brussels, pp. 1-12.

European Council (2020a): "Special meeting of the European Council, Conclusions", European Council Report EUCO 13/20, Brussels.

European Council (2020b): "Decision (CFSP) 2020/1127 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States", European Council Decision OJ L 246/12, Brussels.

European Council (2020c): "Decision (CFSP) 2020/1537 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States", European Council Decisions OJ L 351I, Brussels, pp. 5-7.

European Council (2020d): "Declaration by the High Representative on behalf of the European Union—call to promote and conduct responsible behavior in cyberspace", 21 February 2020 (https://www.consilium.europ a.eu/en/press/press-releases/2020/02/21/declaration-by-the-high-representative-on-behalf-of-the-european-union-call-to-promote-and-conduct-responsible-behavior-in-cyberspace/).

European Parliament and Council (2016): "Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union", European Parliament and Council Directive OJ L 194, Brussels, pp. 1-30.

European Parliament and Council (2019): "Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013) (Text with EEA relevance) PE/86/2018/REV/1", European Parliament and Council Regulation OJ L 151, Brussels, pp. 15-69.

European Presidency (2016): "Non-paper: Developing a joint EU diplomatic response against coercive cyber operations", Non-Paper of the European Presidency 5797/6/16 REV 6, Brussels.

Finnemore, M. B./Hollis, D. (2020): "Beyond naming and shaming: accusations and international law in cybersecurity." In: European Journal of International Law, 2020 forthcoming (https://ssrn.com/abstract=3347958).

Fischerkeller, M. P./Harknett, R. J. (2017): "Deterrence Is Not a Credible Strategy for Cyberspace." In: Orbis 61/3, pp. 381-393.

Franke, U./Varma, T. (2019): "Independence play: Europe's pursuit of strategic autonomy", July 18 (https://www.ecfr.eu/specials/scorecard/independence_play_europes_pursuit_of_strategic_autonomy).

Govaere, I. (2018): "Interconnecting Legal Systems and the Autonomous EU Legal Order: A Balloon Dynamic." In: Research Papers in Law 2/2018, unpaginated.

Greenberg, A. (2017): "How an Entire Nation Became Russia's Test Lab for Cyberwar", June 20 (https://www.wired.com/story/russian-hackers-attack-ukraine/).

Harknett, R. J./Nye, J. S. (2017): "Is Deterrence Possible in Cyberspace?" In: International Security 42/2, pp. 196-199.

ICJ (1997): "The Gabcíkovo-Nagymaros Project (Hungary/Slovakia)", Judgment, International Court of Justice Reports, p. 7.

ILC (2001): "Draft articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries." In: Yearbook of the International Law Commission 2/2, pp. 31-143.

Kelsen, H. (1948): "Collective Security and Collective Self-Defense Under the Charter of the United Nations." In: The American Journal of International Law 42/4, pp. 783-796.

Korzak, E. (2015): "International Law and the UN GGE Report on Information Security", December 2 (https://www.justsecurity.org/28062/international-law-gge-report-information-security/).

Kribbe, H. (2020): "No more Mr. Nice Europe", October 13 (https://www.politico.eu/article/no-more-mr-nice-europe-eu-foreign-policy).

Libicki, M. C. (2009): Cyberdeterrence and Cyberwar, Santa Monica: RAND.

Libicki, M. C. (2017): "It Takes More than Offensive Capability to Have an Effective Cyberdeterrence Posture", Testimony before the House Armed Services Committee, March 1 (https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT465/RAND_CT465.pdf).

Macron, E. (2017): Speech on a New Initiative for Europe, 26 September 2016 (https://www.elysee.fr/emmanuel-macron/2017/09/26/president-macron-gives-speech-on-new-initiative-for-europe.en)

Morgan, P. (2003): Deterrence Now, Cambridge: Cambridge University Press.

Nakashidze, G. (2020): "Cyberattack against Georgia and International Response: emerging normative paradigm of 'responsible state behavior in cyberspace'?", Feburary 28 (https://www.ejiltalk.org/cyberattack-against-georgia-and-international-response-emerging-normative-paradigm-of-responsible-State-behavior-in-cyberspace/).

Nye, J. S. (2017): "Deterrence and Dissuasion in Cyberspace." In: International Security 41/3, pp. 44-71.

Roguski, P. (2020): "Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace", March 6 (https://www.justsecurity.org/69019/russian-cyberattacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace).

Roscini, M. (2015): "Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations." In: Texas International Law Journal 50, pp. 233-273.

Russell, M. (2018): EU sanctions: A key foreign and security policy instrument, Brussels: European Parliamentary Research Service.

Ruys, T. (2016): 'Sanctions, Retorsions and Countermeasures: Concepts and International Legal Framework." In: Larissa van den Herik (ed.), Research Handbook on UN Sanctions and International Law, Cheltenham: Edward Elgar Publishing, pp. 19-51.

Sierzputowski, B. (2019): "The Data Embassy under Public International Law." In: International&ComparativeLawQuarterly 68/1, pp. 225-242.

Schelling, T. C. (2008): Arms and Influence, New Haven: Yale University Press.

Schmitt, M. (2017): The Tallinn Manual 2.0, Cambridge: Cambridge University Press.

Soesanto, S. (2020): "Europe's Incertitude in Cyberspace", August 3 (https://www.lawfareblog.com/europes-incertitude-cyberspace).

Spiro, P. J. (2004): "What Happened to the 'New Sovereigntism'?" In: Foreign Affairs, July 28 (https://www.foreignaffairs.com/articles/united-States/2004-07-28/what-happened-new-sovereigntism).

Taddeo, M. (2018): "The Limits of Deterrence Theory in Cyberspace." In: Philosophy & Technology 31/3, pp. 339-355.

Tamma, P. (2017): "Europe wants 'strategic autonomy'—it just has to decide what that means", Politico, October 15 (https://www.politico.eu/article/europe-trade-wants-strategic-autonomy-decide-what-means).

Timmers, P. (2019): "Strategic Autonomy and Cybersecurity", Policy in Focus (https://eucyberdirect.eu/wp-content/uploads/2019/05/paul-timmers-strategic-autonomy-may-2019-eucyberdirect.pdf).

The Economist (2020): "America rethinks its strategy in the Wild West of cyberspace", May 28 (https://www.economist.com/united-States/2020/05/28/america-rethinks-its-strategy-in-the-wild-west-of-cyberspace).

Quackenbush, S. L. (2011): "Deterrence Theory: Where Do We Stand?" In: Review of International Studies 37, pp. 741-762.

Van den Herik, L. J. (2014): "Peripheral Hegemony in the Quest to Ensure Security Council Accountability for Its Individualized UN Sanctions Regimes." In: Journal of Conflict and Security Law 19/3, pp. 427-449.

Van Reybroeck, R. (2019): "What's in the CARDs?" In: Egmont Security Policy Brief 103, pp. 1-7.

White House (2015): "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities", Executive Order 13694, US Federal Register 80/63, pp. 18077-18079.

White House (2016a): "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities", Executive Order 13757, US Federal Register 82/1, pp. 1-3.

White House (2016b): "Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment", Office of the Press Secretary, December 29 (https://obamawhitehouse.archives.gov/the-pres s-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity).

République Francaise (1994): Livre blanc sur la defense, Paris: La documentation francaise.

Zable, S. (2018): "The Foreign Investment Risk Review Modernization Act of 2018", Law Fare Blog, August 2 (https://www.lawfareblog.com/foreign-investment-risk-review-modernization-act-2018).