digital legal lab

Cybersecurity Conference

JUNE 22, 2023

Brussels

Register here

Abstract Session 1:

Abstract Session 2:

Session 1

Pier Giorgio Chiara (2022): The Emergence of Cybersecurity Law in EU. In: EU Cybersecurity: Collective Resilience through Regulation, June 22nd 2023, Brussels - Belgium

The Emergence of Cybersecurity Law in EU

Pier Giorgio Chiara
University of Bologna, Italy
piergiorgio.chiara2@unibo.it

Extended Abstract

Cybersecurity does not figure as a policy field in the EU Treaties, nor there is an explicit legal basis for EU policy in this regulatory area. Henceforth, the legal basis for EU policy in this area has been predominantly the functioning of the internal market in accordance with Art. 114 TFUE (Odermatt, 2018, p. 359). This article aims to cast light on the emergence of a new policy area in EU law, that is, 'Cybersecurity law' by engaging in the debate on the introduction of a new fundamental right to cybersecurity in EU law (Papakonstantinou, 2022)[1]. Two important legal challenges can be derived from Papakonstantinou's theoretical framework for development of a new right to cybersecurity. They regard: i) the relationship between the concepts of *cybersecurity* and *security,* and, whether the former could be subsumed under the latter; and ii) the actual legal remedies EU cybersecurity law place at the disposal of individuals if cybersecurity threats actually materialise.

As regards the first legal challenge, I will argue that the 'Internet of Things' (IoT), and cyber-physical systems in general, brings about a paradigm shift, for it

[1] On a comparative note see: Kilovaty, 2020; Shackelford, 2019.

intertwines cybersecurity and security (and safety) more than ever before. The IoT blurs the boundaries between the *digital* and the *physical.* IoT ubiquitous computing renders the physical – virtual dichotomy rather anachronistic, as, in the words of Floridi, "we no longer live online or offline but onlife, that is, we increasingly live in that special space, or infosphere, that is seamlessly analogue and digital, offline and online" (Floridi, 2018, p. 1). This increasingly leads to addressing traditional notions of cybersecurity, security and safety in a more interchangeably or unified way (Vedder, 2020, p. 21; Wolf & Serpanos, 2020, pp. 35–36). The assets traditionally protected by cybersecurity and security increasingly overlap. The hyper-connectedness of *every* social sphere, of the market, brought by the IoT shows the dependence of "human safety on encryption, authentication, data integrity, availability, and other dimensions of cybersecurity" (Denardis, 2020, p. 184). Thus, risk factors and threats in today's *digital-physical* environment go beyond the technological infrastructure of information systems, networks and the underlying information. Cyberattacks could also infringe individuals' fundamental rights, impair physical safety and have critical consequences for services, institutions and communities.

Against the background of an increasingly convergence of the concepts of security, cybersecurity and safety, an amendment to the general right to security, namely Article 6 of the EU Charter of Fundamental Rights, or even an extensive interpretation can be suggestive. However, counterarguments can be raised against these two approaches. First, the intricacies behind a revision of EU Treaties (Closa, 2018; Jakab & Kirchmair, 2022, p. 11) suggest that such an approach is unlikely. Second, "the rights in Article 6 are the rights guaranteed by Article 5 of the ECHR […] and they have the same scope"[2]. Art. 5 ECHR – as consistently interpreted by the ECtHR – cannot at present stage be interpreted to include cybersecurity (European Court of Human Rights, 2022).

Beyond primary law questions, there is another issue that ought to be addressed vis-à-vis the reasons for introducing this new right i.e., whether existing (and proposed) secondary legislation grants remedies to individuals if the addressees of EU cybersecurity legislation infringe the legal duties they shall comply with.

---

[2] EXPLANATIONS RELATING TO THE CHARTER OF FUNDAMENTAL RIGHTS (2007/C 303/02), Official Journal of the European Union, p. 3.

The NIS Directive[3], the new NIS2 Directive[4] and the Cybersecurity Act[5] do not afford any rights nor remedies to individuals, as they address the security of network and information systems and the EU cybersecurity certification framework respectively. These legal acts have thus their primary objectives in the 'functioning of the internal market' and not the protection of natural and/or legal persons *per se*. Against this backdrop, the article will predominately focus on the legal analysis on the Commission's proposal for a 'Cyber Resilience Act' (CRA)[6], which importantly will introduce a set of ex-ante and ex-post cybersecurity obligations for all economic operators throughout the supply chain of products with digital elements. Indeed, the CRA aims to enhance the overall level of cybersecurity of hardware and software products in the Single Market as cybersecurity incidents can, in fact, impact the health and safety of users. This line of reasoning is explicitly endorsed by Art. 10(2) CRA proposal, which lays down various obligations of manufacturers[7]. It follows that the argument previously made regarding the increasingly blurred distinction between the concepts of cybersecurity and security holds.

From a law-making perspective, a new right to cybersecurity seems to be misplaced even in the Cyber Resilience Act, because of its anchoring in product safety legislation (Chiara, 2022). Unsurprisingly, the CRA finds its legal basis in Art. 114 TFEU, like the NIS Directive(s) and the Cybersecurity Act. And just as the two latter legal acts, the CRA proposal does not provide any remedies for individuals, contrary to the expectations of the EU consumer association BEUC (BEUC, 2022, p. 12). In this regard, it should be worth exploring the synergies between the CRA, which does not address liability issues, and the newly proposed

---

3 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

4 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

5 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

6 Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.

7 "Manufacturers shall undertake an assessment of the cybersecurity risks associated with a product with digital elements […] with a view to minimising cybersecurity risks, preventing security incidents and minimising the impacts of such incidents, including in relation to the health and safety of users".

Directive on liability for defective products[8] for it will deem a product to be defective when it does not provide *inter alia* safety-relevant cybersecurity requirements which the public at large is entitled to expect (Art. 6(1)(f) Directive on liability for defective products proposal.). These cybersecurity requirements are laid down in the CRA (Recital 16 CRA) and – where the CRA does not apply – in the proposed General Product Safety Regulation (Recital 22; Art. 5a(1)(h) GPSR)[9]. In other words, the new legal framework that the Directive on liability for defective products introduces will provide individuals with remedies and means of redress if a cybersecurity vulnerability of a product is exploited and, accordingly, damages occur.

Eventually, a new right to cybersecurity would best guide the fast-growing regulatory landscape and support the emergence of the new policy field of EU cybersecurity law (Wessel, 2015). EU cybersecurity law has shifted relatively recently, that is, from the adoption of the Cybersecurity Act in 2019, from organisational and technical legislation to a comprehensive multi-level and multi-stakeholder regulatory approach (European Commission and the High Representatitve of the Union for Foreign Affairs and Security Policy, 2020, p. 23)[10]. If introduced at some point in EU secondary law, a new right should reflect the *holistic* approach to cybersecurity enshrined in the broad definition provided by Art. 2(1) Cybersecurity Act, which includes all the "activities necessary to protect network and information systems, *the users of these systems and other persons affected by cyberthreats*". This, in turn, would facilitate the affordance of legal remedies, including insurance schemes, for individuals if a cybersecurity threat materialises in an incident and, consequently, damages occur outside the scope of products safety legislation.

---

8 Proposal for a Directive of the European Parliament and of the Council on liability for defective products.

9 Proposal for a Regulation of the European Parliament and of the Council on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council, EU Parliament provisional agreement, 21.12.2022.

10 Cybersecurity is increasingly seen as a shared responsibility between the public sector, which has to provide the relevant legal frameworks, the private sector, which has to design and place in the market products with effective cybersecurity and regular users, which will be asked to observe so-called 'cyber-hygiene practices' (Brighi & Chiara, 2021; Taddeo, 2019).

References

BEUC. (2022): *Cyber Resilience Act: Cybersecurity of Digital Products and Ancillary Services - BEUC response to public consultation*. https://www.beuc.eu/publications/beuc-x-2022-051_cyber_resilience_act_public_consultation_beuc_position_paper.pdf.

Brighi, R., & Chiara, P. G. (2021): 'La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea', *Federalismi.It*, vol. 21, pp. 18–42.

Chiara, P. G. (2022): 'The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements', *International Cybersecurity Law Review* , vol. 3, issue 2 , pp. 255–272.

Denardis, L. (2020): *The Internet in Everything - Freedom and Security in a World with No Off Switch* (1st ed.), Yale University Press.

European Commission and the High Representatitve of the Union for Foreign Affairs and Security Policy. (2020): *Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade.*

European Court of Human Rights. (2022): *Guide on Article 5 of the European Convention on Human Rights: Right to liberty and security*. https://www.echr.coe.int/Documents/Guide_Art_5_ENG.pdf

Floridi, L. (2018): 'Soft Ethics and the Governance of the Digital', *Philosophy & Technology*, vol. 31, pp. 1–8.

Jakab, A., & Kirchmair, L. (2022): 'Two Ways of Completing the European Fundamental Rights Union: Amendment to vs. Reinterpretation of Article 51 of the EU Charter of Fundamental Rights', *Cambridge Yearbook of European Legal Studies*, vol. 23, pp. 1–23.

Kilovaty, I. (2020): 'An Extraterritorial Human Right to Cybersecurity', *Notre Dame Journal of International & Comparative Law*, vol. 10, pp. 35–55.

Odermatt, J. (2018): 'The European Union as a Cybersecurity Actor', in S. Blockmans & P. Koutrakos (eds.), *Research Handbook on EU Common Foreign and Security Policy*, Edward Elgar Publishing, pp. 354–373.

Papakonstantinou, V. (2022): 'Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity?', *Computer Law and Security Review*, vol. 44, issue 105653, pp. 1-15.

Shackelford, S. J. (2019): 'Should Cybersecurity be a Human Right? Exploring the "Shared Responsibility" of Cyber Peace', *Stanford Journal of International Law*, vol. 55, issue 2, pp. 158–184.

Taddeo, M. (2019): 'Is Cybersecurity a Public Good?', *Minds and Machines*, vol. 29, issue 3, pp. 349–354.

Vedder, A. (2020): 'Safety, Security and Ethics', in A. Vedder, J. Schroers, C. Ducuing, & P. Valcke (eds.), *Security and Law*, Cambridge, Antwerp, pp. 11–26.

Wessel, R. A. (2015): 'Towards EU cybersecurity law: Regulating a new policy field', in N. Tsagourias & R. Buchan (eds.), *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing Ltd, pp. 403–425.

Wolf, M., & Serpanos, D. (2020): *Safe and Secure Cyber-Physical Systems and Internet-of-Things Systems,* Springer.

Mattis van 't Schip (2022): Open-Source Software Development and the Cyber Resilience Act: Digital Altruism versus Commerciality. In: EU Cybersecurity: Collective Resilience through Regulation, June 22nd 2023, Brussels - Belgium

Open-Source Software Development and the Cyber Resilience Act: Digital Altruism versus Commerciality

Mattis van 't Schip
Ph.D. Candidate, Radboud University (iHub)
mattis.vantschip@ru.nl

Abstract

Our modern digital infrastructure largely runs on open-source software. The source code of this type of software is freely accessible, shareable, and modifiable for any developer or other end user. Many routers run on the OpenWRT operating system, while many laptops and PCs run the Linux operating system. Both systems are fully open source.

Due to its integral role in modern digital infrastructure, any security vulnerabilities in open-source software have equally significant effects when compared to their 'closed-source' counterparts. The Director of the US Cybersecurity Agency (CISA) called a recent vulnerability in a piece of open source logging software 'one of the most serious vulnerabilities' she had encountered in her career (Lyngaas, 2021).

Meanwhile, developers maintain their open-source software packages based on personal passion or similar altruistic motivations (Bitzer et al., 2007). They often receive little to no remuneration for their work.

European legislation has thus far left questions surrounding open-source software vulnerabilities outside its scope. The recent proposal for the Cyber Resilience Act brings a central change to this landscape, as the Commission specifically addresses free and open-source software in this new set of security rules for digital products. At first sight, the Commission fully exempts open-source

software from the scope of the Act. A closer look, however, shows that the Commission exempts open-source software only when it is not developed within the course of a 'commercial activity'. In this paper, I focus on this conditional exemption and compare it with other approaches in the European legal framework for digital products. The aim of this comparative analysis is to find a model of responsibilities that aligns both with the aims of the Cyber Resilience Act and the characteristics of open-source software. I will answer the following question: *'To what extent are alternatives models required for the Cyber Resilience Act proposal to bring its obligations in line with the particularities of open-source software, when compared with other approaches in the European legal framework for digital products?'* In answering this question, I argue that the Cyber Resilience Act should shift towards a model based on the altruistic—instead of the commercial—aspects of open-source software.

The Cyber Resilience Act and Open-Source Software

The Cyber Resilience Act proposal introduces a set of cybersecurity requirements for virtually all software and hardware products that enter, or are used within, the European Union. The security requirements of the Act mainly apply to the 'manufacturer' of a product, a definition that also includes the developer of software. The requirements are extensive, ranging from security practices and measures that the product must comply with (e.g., security-by-default, confidentiality of data), to product safety measures that the manufacturer must implement (e.g., technical documentation, vulnerability patching).

For open-source software, many of the security requirements and safety measures are not new. Security research has shown that open-source and closed source software do not significantly differ in levels of security (Meneely and Williams, 2009). The onus for open-source software lies in the product certification process of the Cyber Resilience Act. The Act distinguishes between three levels of products: normal products; critical products (e.g., network logging software); and highly critical products (adopted later by Commission through implementing acts). For the latter two levels, the Act requires a more extensive security assessment procedure. Where developers of 'normal' products can perform a self-assessment to determine whether they meet the requirements of the Act, developers of critical and highly critical products must arrange a third-party assessment. Open-source software often has certain elevated privileges within a network or device (e.g., Log4Shell for network logging purposes, Bitwarden for password management), making the product critical and thus requiring a third-party assessment for compliance with the CRA. This assessment procedure is too intensive for open source software developers when compared to the altruistic nature of their work: assigning a third-party auditor is probably too expensive for many developers (Aertsen, 2022).

In theory, the Cyber Resilience Act exempts open-source software from its scope if the software is not offered in 'the course of a commercial activity' and

therefore the Act has no impact on open-source software development. In the context of open-source software, the Act specifies a few examples of a commercial activity: 1) charging a price for the software; 2) charging a price for technical support; 3) providing a software platform where other services are monetised (e.g., Android, which is open source at its core, with Google applications). This list is not exhaustive and thus other cases of a commercial activity are possible. The EU 'Blue Guide' states that a commercial activity can only be assessed on a case-by-case basis by taking into account, for instance, the regularity of supplies and the intentions of the supplier (European Commission, 2022). This case-by-case assessment allows for flexibility, as defining a 'commercial activity' for each business practice is not possible. In the context of open-source software, however, many types of funding and income exist, ranging from offering technical support for monthly fees to allowing end users to make small donations (Wheeler, 2009). The ambiguity surrounding the 'commercial activity' condition might thus deter the open-source software developer from continuing the maintenance of their product in face of possible legal procedures. The Cyber Resilience Act's exemption for open-source software development, therefore, leaves many lingering questions.

The Role of Open-Source Software in the European Legal Framework

The commercial activity condition in the Cyber Resilience Act exists within the wider European legal framework. The recent proposal for a new Product Liability Directive employs the commercial activity condition for open-source software, while the Unfair Commercial Practices Directive (UCPD) has included the concept since 2005.[1]

The recent Product Liability Directive (PLD) proposal includes a similar exemption for open-source software as the Cyber Resilience Act. The Commission is thus strongly embedding the exemption in the new European product legislation framework. The PLD re-iterates the approach in the Cyber Resilience Act, but also takes a slightly different approach to the commercial activity condition. For instance, the PLD states that products supplied in the context of a 'service financed by public funds' have an economic character and are, therefore, offered in the course of a commercial activity. As more public institutions are adopting open source software, the 'public funding' example thus brings an additional option for offering open-source software in the course of a commercial activity (European Data Protection Supervisor, 2023).

[1]In the first iterations of the Directive, the definition was 'commercial practice'.

The 'commercial activity' in the UCPD differs significantly from its twin in the Cyber Resilience Act. In the UCPD, a commercial activity requires certain marketing or communication acts or omissions that stand in direct relation to the

promotion, sale, or supply of a product from a trader towards a consumer. This means that the commercial activity must stand in direct relation to pre-contractual marketing and business strategies (Anagnostaras, 2010). In comparison, the commercial activity in the CRA covers any type of action, at any stage of the development process, that might bring the software into the 'business-related context'.

The commercial activity condition is thus rather ambiguous within the European legal framework, which might prove problematic for open-source software development. An alternative that shifts away from this ambiguous condition might thus prove more future-oriented and applicable (Wheeler, 2009).

I argue for open-source software development as a form of 'altruism' (Maxwell, 2006). The European legislators recently introduced 'data altruism' options for organisations that aim to provide data for altruistic purposes (e.g., for research) in the Data Governance Act. A close examination of the 'open source' community and wider movement indicate certain close correlations with the data altruism efforts(e.g., by providing software to the public to support efforts of public interest). A model based on the existence of altruism, instead of the absence of commerciality, might prove more aligned with the benefits of open-source software development and the security aims of the Cyber Resilience Act.

From Absence of Commerciality to Existence of Altruism

The altruism-based model offers several recommendations that benefit the developers of open-source software and the cybersecurity aims of the Cyber Resilience Act. The Data Governance Act requires that data altruism organisations implement security measures in their data processing as part of the certification process. There is thus an imaginable link between the security aims of the Cyber Resilience Act and a model for open-source software based on 'digital altruism'.

A new approach in the Cyber Resilience Act must also consider the barriers imposed to altruistic organisations, as evident from the many requirements in the Data Governance Act. NGOs have argued that the Data Governance Act merely adds additional bureaucratic layers for altruistic organisations and therefore might prove wholly ineffective (Veil, 2021). Such considerations also lie at the foundation of criticism on the Cyber Resilience Act and thus are taken into account in the proposed model.

The 'digital altruism' model, in turn, offers well-informed recommendations on how altruism, instead of commerciality, must lie at the foundation of product cybersecurity rules for open-source software.

References

Aertsen, M. (2022, November 14): Open-source software vs. The proposed Cyber Resilience Act.

The NLnet Labs Blog. https://blog.nlnetlabs.nl/open-source-software-vs-the-cyber-resilience act/.

Anagnostaras, G. (2010): 'The Unfair Commercial Practices Directive in Context: From Legal Disparity to Legal Complexity?', *Common Market Law Review*, vol. 47, no. 1, February 2010, pp. 147–171. https://doi.org/10.54648/COLA2010006.

Bitzer, J., Schrettl, W., and Schröder, P. J. H. (2007): 'Intrinsic motivation in open source software development', *Journal of Comparative Economics*, vol. 35, no. 1, March 2007, pp. 160–169. https://doi.org/10.1016/j.jce.2006.10.001.

European Commission (2022, June 29): Blue Guide for the implementation of product legislation. https://eur-lex.europa.eu/legal content/EN/TXT/PDF/?uri=OJ:C:2022:247:FULL&from=EN.

European Data Protection Supervisor (2023, February 23): EDPS to pilot the use of Open Source Software. https://edps.europa.eu/press-publications/press-news/press-releases/2023/edps pilot-use-open-source-software_en.

Lyngaas, S. (2021, December 13): US warns hundreds of millions of devices at risk from newly revealed software vulnerability. CNN. https://www.cnn.com/2021/12/13/politics/us-warning software-vulnerability/index.html.

Maxwell, E. (2006): 'Open Standards, Open Source, and Open Innovation: Harnessing the Benefits of Openness', *Innovations: Technology, Governance, Globalization*, vol. 1, no. 3, July 2006, pp. 119–176. https://doi.org/10.1162/itgg.2006.1.3.119.

Meneely, A., and Williams, L. (2009): 'Secure open source collaboration: An empirical study of linus' law', *Proceedings of the 16th ACM Conference on Computer and Communications Security*, November 2009, pp. 453–462. https://doi.org/10.1145/1653662.1653717

Veil, W. (2021): Data altruism: How the EU is screwing up a good idea. Algorithm Watch. https://algorithmwatch.org/de/wp content/uploads/2022/01/2022_AW_Data_Altruism_final_publish.pdf.

Wheeler, D. A. (2009): F/LOSS is Commercial Software. In Open Source Business Resource. Talent First Network. http://timreview.ca/article/229.

Eyup Kun (2022): Searching for the appropriate legal basis for personal data processing in the realm of NIS 2 Directive: Legitimate Interest or Legal Obligation?. In: EU Cybersecurity: Collective Resilience through Regulation, June 22nd 2023, Brussels - Belgium

Searching for the Appropriate Legal basis for Personal Data Processing in the Realm of the NIS 2 Directive: Legitimate Interest or Legal Obligation?

Eyup Kun
Doctoral Researcher, KU Leuven Center for IT and IP Law
eyup.kun@kuleuven.be

Abstract

The NIS 2 Directive, in its final version, explicitly stipulates the possibility of legal obligation as a legal basis for the processing of personal data for cybersecurity purposes. Art. 2(14) of the final version of the NIS 2 Directive states that entities must process personal data to the extent necessary for this Directive and per GDPR, specifically Art. 6. As a clarification, Recital 121 of the NIS 2 Directive stipulates that essential and important entities may process personal data to the extent necessary and proportionate to secure network and information systems following Art. 6(1), point (c) of the GDPR.

Considering the stipulation of the possibility of legal obligation for personal data processing for cybersecurity purposes under the NIS 2 Directive, this paper examines the question of whether it is appropriate to use legal obligation as a legal basis by important and essential entities when they process personal data. In addition, this paper discusses how legal obligation as a legal basis for personal data processing should be established following the standards mentioned in Recital 41 and Recital 45 of the GDPR.

The extended abstract has three main sections. First, it provides a general context of how ensuring cybersecurity might conflict with the objective of the right to personal data protection. Second, it briefly discusses the potential legal basis for cybersecurity purposes. Third, it reiterates the research question that the proposed paper will respond to and the contribution the proposed paper makes to legal scholarship.

1. Considering the intricate relationship between cybersecurity and data protection while deciding the appropriate legal basis

The NIS 2 Directive is inextricably linked with the GDPR. On the one hand, the GDPR imposes security responsibilities upon data controllers and data processors. Similarly, NIS 2 Directive requires important and essential entities to take technical and organizational measures to ensure cybersecurity during their operations.

On the other hand, the objective of ensuring cybersecurity might compromise the right to personal data protection. This conflict can be seen in particular when processing and collecting personal data of natural persons, such as IP addresses of website users is needed to ensure cybersecurity. For instance, Naarttijärvi shows how the cybersecurity objective can conflict with the right to data protection by analysing the example of information security sensor systems in Sweden, which requires invasive network monitoring techniques (Naarttijärvi, 2018). In another example, Greitzer and Hohimer propose modelling human behaviour to anticipate insider attacks to ensure cybersecurity (Greitzer & Hohimer, 2011). They propose to process keystroke records, email content capture, and email headers to anticipate insider attackers to prevent cybersecurity(Greitzer & Hohimer, 2011). This information can be considered as personal data and this modelling can be considered as invasive as it creates a profile of an employee to decide whether they can be considered an insider attacker. Thus, these examples show that the relationship between the right to data protection as a fundamental right and the overall objective of cybersecurity is not clear-cut and requires a tuned approach.

2. Searching for the legal basis for cybersecurity purposes under the GDPR

When personal data is processed for cybersecurity purposes, this processing shall be done on a legal basis. The tuned approach is in particular required for choosing the legal basis for cybersecurity purposes. While the GDPR does not require a legislative act adopted by parliament unless the member state constitutional order requires it, Recital 41 requires the legal basis to be clear and precise, and its

application to persons subject to it to be foreseeable. The GDPR explicitly refers to case law from the CJEU and the ECtHR in this context. Recital 45 adds that this legal basis 'could' specify the conditions of processing under the GDPR, as well as specifications regarding, among other things, the type of data subject to processing, entities to which the personal data may be disclosed, purpose limitations, storage periods, and 'other measures to ensure lawful and fair processing'. For cybersecurity purposes, the most relevant legal grounds might be consent (Art. 6(1)(a), the legal obligation (Art. 6(1)(c), the necessity for the performance of a task carried out in the public interest (Art. 6(1)(e) as well as a legitimate interest (Art. 6(1)(f).

Regarding consent as a legal basis, consent may not be an appropriate legal basis for ensuring cybersecurity for two reasons. First, data subjects can revoke consent at any time under Art. 7(3) of the GDPR((Albakri et al., 2019; Sullivan & Burger, 2017). This dependency may make the legality of the processing of personal data uncertain.

Regarding reliance on the public interest under Art. 6(1) e, according to this provision, ‘’personal data shall be processed if the processing is necessary for the performance of a task carried out in public interest or the exercise of official authority vested in the controller’’. By conceptualising information-sharing in the public interest, Sullivan and Burger argued that data controllers can rely on that legal basis when they deploy automated sharing of IP addresses(Sullivan & Burger, 2017). Considering the importance of information sharing for collectively defending the cyber-sphere, it is true that information sharing indeed falls within the scope of public interest. However, I do not agree with Sullivan and Burger on the reliance on Art. 6(1)e on the following reasoning. It is unclear whether the words 'vested in the controller' refer to 'exercise of official authority' or 'a task' in the English version of Art. 6(1)(e)(Kotschy, 2020). As Kotchy argues that the German version, where commas are used to structure the sentence, clarifies the meaning. This structure would be translated into English as follows: 'Processing is required for the performance of a task carried out in the public interest or the exercise of official authority vested in the controller'. However, Sullivan seems to interpret the first element `processing is necessary for the performance of a task carried out in public interest` without considering the second element `vested in the controller` (Kotschy, 2020). Therefore, as long as entities as data controllers are not vested in a task of information-sharing with other entities, they cannot rely on the Art. 6(1)(e).

Regarding the legitimate interest, personal data processing is lawful only if it is required for the controller's or a third party's legitimate interests unless such interests are overridden by the data subject's interests, fundamental rights and freedoms according to Art. 6(1)(f). Some scholars argue that overriding legitimate interest can be a legal basis for such processing, however, they also contended that, due to the lack of guidance in legislation and case law, it is unclear how data controllers can depend on such a legitimate interest (Cole & Schmitz, 2019;

Didenko, 2020). As a result, that provision establishes three cumulative conditions for the lawfulness of personal data processing: the pursuit of a legitimate interest by the data controller or a third party, the need to process personal data for the legitimate interests pursued; and the interests, freedoms, and fundamental rights of the person concerned by data protection do not take precedence. Cybersecurity is one of the legitimate interests explicitly recognised under Recital 49 of the GDPR for providers of security technologies and services. In particular, data controllers inevitably process personal data for the prevention, detection and investigation of security incident security (*CIPL Publishes White Paper on How the Legitimate Interest Ground for Processing Enables Responsible Data Use and Innovation*, 2021). Cormack discovered a strong alignment and proposed pertinent factors for the legitimate interests balancing test to guarantee that the interests of users were protected when they shared information (Cormack, 2021). Similarly, Bakri and others argued for the appropriateness of legitimate interest by proposing data protection by design approach to balance the interests of data subjects and the interest to share information (Albakri et al., 2019; Maltzan, 2019).

3. Processing of Personal Data for Cybersecurity under the NIS 2 Directive: Legal Obligation or Legitimate Interest?

The final version of the NIS 2 Directive explicitly states the possibility of legal obligation as a legal basis for the processing of personal data for cybersecurity purposes. According to Art. 2(14) of the final version of the NIS 2 Directive, entities must process personal data to the extent required for this Directive and GDPR, specifically Art. 6. Recital 121 of the NIS 2 Directive states that essential and important entities may process personal data to the extent necessary and proportionate to secure network and information systems following Regulation (EU) 2016/679, Art. 6(1), point (c), and Art. 6(3). Considering the NIS 2 Directive's stipulation of legal obligation for personal data processing for cybersecurity purposes, this paper investigates whether it is appropriate for important and essential entities to use legal obligation as a legal basis. Furthermore, this paper discusses how legal obligations as the legal basis for personal data processing should be established per the standards mentioned in GDPR Recitals 41 and 45. This article adds to the legal literature by the examination of the implications of the processing of personal data on legitimate interest and legal obligation for cybersecurity purposes by important and essential entities in light of the change in the NIS 2 Directive. It proposes the use of legitimate interest as a legal basis rather than a legal obligation and recommends Member States not establish a legal obligation as a legal basis for processing personal data for cybersecurity purposes when they transpose the NIS 2 Directive to their national laws.

References

Albakri, A., Boiten, E., & Lemos, R. (2019). *Sharing Cyber Threat Intelligence Under the General Data Protection Regulation* (pp. 28–41). https://doi.org/10.1007/978-3-030-21752-5_3

CIPL Publishes White Paper on How the Legitimate Interest Ground for Processing Enables Responsible Data Use and Innovation. (2021, July 21). Privacy & Information Security Law Blog. https://www.huntonprivacyblog.com/2021/07/21/cipl-publishes-white-paper on-how-the-legitimate-interest-ground-for-processing-enables-responsible-data-use-and innovation/

Cole, M. D., & Schmitz, S. (2019). *The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape* (SSRN Scholarly Paper No. 3512093). https://doi.org/10.2139/ssrn.3512093

Cormack, A. (2021). NISD2: A Common Framework for Information Sharing among Network Defenders. *SCRIPTed: A Journal of Law, Technology and Society*, *18*(1), 83–98.

Didenko, A. N. (2020). Cybersecurity regulation in the financial sector: Prospects of legal

harmonization in the European Union and beyond. *Uniform Law Review*, *25*(1), 125–167. https://doi.org/10.1093/ulr/unaa006

Greitzer, F., & Hohimer, R. (2011). Modeling Human Behavior to Anticipate Insider Attacks. *Journal of Strategic Security*, *4*(2). http://dx.doi.org/10.5038/1944-0472.4.2.2

Kotschy, W. (2020). Article 6 Lawfulness of processing. In *Article 6 Lawfulness of processing*. Oxford University Press. https://doi.org/10.1093/oso/9780198826491.003.0035

Maltzan, S. von. (2019). No Contradiction Between Cyber-Security and Data Protection? Designing a Data Protecton Compliant Incident Response System. *European Journal of Law and Technology*, *10*(1). https://ejlt.org/index.php/ejlt/article/view/665

Naarttijärvi, M. (2018). Balancing data protection and privacy – The case of information security sensor systems. *Computer Law & Security Review*, *34*(5), 1019–1038. https://doi.org/10.1016/j.clsr.2018.04.006

Sullivan, C., & Burger, E. (2017). "In the public interest": The privacy implications of international business-to-business sharing of cyber-threat intelligence. *Computer Law & Security Review*, *33*(1), 14–29. https://doi.org/10.1016/j.clsr.2016.11.015

Zaira Zihlmann (2023): The Proposed EU Cyber Resilience Act from a Digital Sovereignty Perspective. In: EU Cybersecurity: Collective Resilience through Regulation, June 22nd 2023, Brussels – Belgium

The Proposed EU Cyber Resilience Act from a Digital Sovereignty Perspective

Zaira Zihlmann
University of Lucerne, Switzerland
zaira.zihlmann@unilu.ch

Abstract

This contribution examines the proposed EU Cyber Resilience Act (CRA) by first outlining some of its key aspects before looking at it from the perspective of the notion of digital sovereignty. This examination conceptualizes the EU's quest for digital sovereignty as one of the drivers for the CRA and raises the question whether the CRA could indeed contribute to strengthening the digital sovereignty of the EU.

The Proposal for a Cyber Resilience Act

"If everything is connected, everything can be hacked." (von der Leyen, 2021). With this statement in her 2021 State of the Union Address, European Commission President Ursula von der Leyen pointed to the problem that the emergence of the Internet of Things (IoT) presents a focal point of cybersecurity challenges in the EU. The IoT brings about the integration of devices into networks via their connections to the Internet and to other devices (Weber & Studer, 2016). Yet, many of these devices have low levels of cybersecurity (Carr & Lesniewska, 2020). The widespread use of such devices raises serious concerns as more unsecured devices also mean an extended attack surface and increased cybersecurity risks for their users (Banasiński & Rojszczak, 2021). In addition, the strong cross-border nature of connected devices can cause an incident that initially affects a single entity or

Member State to spread across organizations, industries, and multiple Member States within minutes (Impact Assessment, 2022).

Recognizing this problem, the EU stated in its Cybersecurity Strategy for the Digital Decade[1] that it intends to address this by incentivizing the creation of an Internet of Secure Things and announced new horizontal rules to improve the cybersecurity of products with digital elements that are placed on the internal market (Car & De Luca, 2022). Indeed, the proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, also known as the Cyber Resilience Act (CRA)[2], advanced rapidly and was adopted by the Commission on 15 September 2022[3].

The CRA aims to harmonise and streamline the EU's fragmented cybersecurity regulatory landscape so as to avoid regulatory fragmentation and to ensure a coherent cybersecurity framework. Yet, the main issues the CRA aims to address are the low levels of cybersecurity of products with digital elements and the common inability of users to select products with adequate cybersecurity properties or use them in a secure manner due to insufficient understanding and lack of access to information.[4]

Broadly speaking, these problems are to be tackled by imposing mandatory essential security requirements for all products with digital elements and requiring that the products are secure along the supply chain and throughout their life-cycle, as well as by improving transparency in various aspect so as to enable users to take a product's cybersecurity into account (Burri & Zihlmann, 2023).

In more concrete terms, the CRA comes with a very broad scope of application in that it covers basically all products with digital elements (Chiara, 2022). It is the placing on the EU market that triggers the CRA's application, i.e., the CRA applies to products that are offered for sale or use in the Union (Burri & Zihlmann, 2023). The CRA addresses the economic operators involved in the supply chain of such products (manufacturers, distributors, and importers) and imposes several obligations on them both before and during the placing on the market of a product with digital elements (Car & De Luca, 2022). Particularly manufacturers bear a variety of obligations: Inter alia, when placing a product on the market, they are obliged to ensure that it has been designed, developed and manufactured in accordance with the essential security requirements listed in Annex I Section 1 of the CRA and that the product is not delivered with known exploitable vulnerabilities[5] – hence, the CRA follows the principle of 'security by design' and makes it mandatory (Schmitz-Berndt & Cole, 2022). Moreover, manufacturers must implement vulnerability handling processes to ensure the cybersecurity of a product after it is marketed, for instance by providing security updates.[6] Also, the

---

[1] Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final, 16 December 2020 [hereinafter EU Cybersecurity Strategy].

[2] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, Brussels, 15.9.2022, COM(2022) 454 final, [hereinafter CRA or CRA Proposal].

[3] It should be noted that the subsequent observations mainly refer to the proposal of 15 September 2022. At the time of writing, it is reported that the Swedish Presidency of the EU Council of Ministers has revised the entire proposal (Bertuzzi, 2023).

[4] Explanatory Memorandum to the CRA Proposal.

[5] Art. 10(1) and (6) CRA Proposal.

[6] Art. 10(6) CRA Proposal.

manufacturer carries certain documentation, information, and reporting obligations.[7]

While all products with digital elements must meet the essential cybersecurity requirements of Annex I, they are subject to different conformity assessment procedures, depending on their classification (Chiara, 2022). Based on their level of risk, products are split in two main categories: (1) default 'non-critical products', i.e., hardware and software with a low level of criticality and (2) 'critical products' (Car & De Luca, 2022). The latter being divided into class I and class II products.[8] Consequentially, the CRA follows a risk-based approach with varied regulatory burden not only across types of actors but also types of products.

Furthermore, the CRA grants the EU Commission, ENISA as well as national market surveillance authorities comprehensive market surveillance, investigation, and ordering competences. For instance, they can order an economic operator to take all necessary measures to make a product compliant, to withdraw it from the market or to recall it.[9] Even where products comply with the CRA, authorities have the power to intervene and establish corrective or restrictive measures.[10] It is also possible that several authorities agree to conduct joint activities to verify compliance and identify product cybersecurity risks, such as through so-called "sweeps".[11] In case of non-compliance with the CRA, the market surveillance authorities may impose significant fines akin to those of the GDPR's[12] fine model (Zirnstein et al., 2022). It is not just the fine model that shows similarities to the GDPR; the CRA is reminiscent of the GPDR in other aspects too, which is why the CRA might arguably be described as the "GDPR for IoT" (Gregersen, 2022).

Digital Sovereignty as a Driver of the Cyber Resilience Act

Yet the CRA's provisions outlined above are not only intended to enable an Internet of Secure Things, but should also be put in the context of the EU's efforts to strengthen its digital sovereignty (Burri & Zihlmann, 2023).

The term digital sovereignty, however, lacks a clear definition and is used inconsistently in EU policy documents (Pohle & Thiel, 2020). Indeed, even essential elements are unclear, such as whether digital sovereignty is something that the EU already has, or whether it is a goal that the EU should aspire to (Roberts et al., 2021). Nevertheless, 'digital sovereignty', sometimes referred to as 'technological sovereignty', has been constituted as a specific, explicit policy of the EU Commission since 2019 (Farrand & Carrapico, 2022; Bellanova et al., 2022).

In order to examine the CRA from the perspective of digital sovereignty, this contribution draws on the understanding of digital sovereignty by Roberts et al. and Floridi, where digital sovereignty is *"a form of legitimate, controlling authority"* (Roberts et al., 2021, p. 6) over *"data, software (e.g. AI), standards and protocols*

[7] Art. 10(10), Art. 11 and Art. 23 CRA Proposal.

[8] Art. 6(1) CRA Proposal.

[9] Art. 43(1), (4) and (5) CRA Proposal.

[10] Art. 46 CRA Proposal.

[11] Art. 48 and Art. 49(1) CRA Proposal.

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ (2016) L 119/1 [hereinafter GDPR].

(e.g. 5G, domain names), processes (e.g. cloud computing), hardware (e.g. mobile phones), services (e.g. social media, e-commerce), and infrastructures (e.g. cables, satellites, smart cities)" (Floridi, 2020, p. 370).

Cybersecurity appears as a pillar of EU's digital sovereignty, as strong cybersecurity is seen as a prerequisite for other policy areas, since the security of data, infrastructure and economic entities is necessary for a functional and competitive EU digital economy as well as for the safeguarding of EU values (Roberts et al., 2021). Accordingly, the digital sovereignty discourse points to the EU's considerable dependence on foreign digital infrastructure and service providers, which makes it difficult to provide EU citizens with a high level of cybersecurity, and it emphasises the EU's need to regain control over the digital infrastructure (Farrand & Carrapico, 2022). Consequentially, the EU refocused its cybersecurity-related policies and initiatives around the idea of sovereignty (Barrinha & Christou, 2022), which is reflected in the EU Cybersecurity Strategy that highlights technological sovereignty as one of its key domains and considers the upcoming decade as the *"EU's opportunity to lead in the development of secure technologies across the whole supply chain."*[13]

There are various legislative initiatives that seek to strengthen the EU's digital sovereignty by making it a standard-setter in the field of cybersecurity, such as the NIS2 Directive[14], the Cybersecurity Act[15] as well as the GDPR (Madiega, 2020; Barrinha & Christou, 2022). This also seems to hold true for the CRA, notably since Thierry Breton (2021), the Commissioner for the Internal Market, stated that ensuring EU technological sovereignty in the cyber domain requires regulatory action to enhance the level of security in the internal market by establishing common European cybersecurity standards for products and services, which is what the CRA is designed to do. This intention seems to be reaffirmed in the recently published CRA Draft Report of the Committee on Industry, Research and Energy, which proposes to extend Recital 5 of the CRA to include the following: *"In order for the Union to play a leading international role in the field of cybersecurity, it is important to establish an ambitious overarching regulatory framework."* (Draft Report, 2023, p. 9).

Accordingly, the above-mentioned similarities of the CRA to the GDPR do not appear to be coincidental. Rather, the EU seems to be deliberately attempting to mimic the GDPR, respectively its effects. This might not be an aberrant approach, as it can be argued that the EU's standard-setting role in data protection can serve as a model for the standard-setting role it seeks to have in all areas of cyberspace, especially in the field of cybersecurity (Bendiek & Pander Maat, 2019).

---

[13] EU Cybersecurity Strategy, p. 5.

[14] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ (2022) L 333/80 [hereinafter NIS2 Directive].

[15] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology

The Cyber Resilience Act as an Enabler for Digital Sovereignty?

Still, striving for more digital sovereignty via the CRA by no means ensures that the CRA will contribute to this objective. That being said, the question is how to assess whether a regulatory initiative contributes to the pursuit of digital sovereignty. Criteria that would allow a conclusive assessment of whether a regulation contributes to the realization of digital sovereignty, however, are missing (Kaloudis, 2022). Nonetheless, there are at least some aspects that indicate how digital sovereignty evolves and one may also draw conclusions informed by other regulations, notably the GDPR.

With respect to cybersecurity, both Broeders et al. (2023) as well as Roberts et al. (2021) argue that digital sovereignty unfolds through the exercise of different degrees of authority and control. Meanwhile, Soare (2022) construes digital sovereignty around four principles: (1) Act, i.e., the EU's ability to act free of dependencies in its international relations. (2) Access, which means, inter alia, the EU's ability to constrain non-EU parties' access to its market and technologies. (3) Cooperation, i.e., the EU's openness to engage in international cooperation and multilateralism. (4) Ownership, meaning the EU's ability to control critical technologies and their supply chains. Similar aspects are formulated by Savin (2022), who identifies three elements of digital sovereignty: (1) The territorial scope, whereby this element encompasses the question of whether EU legislation applies extraterritorially. (2) The extent to which the EU is able to regulate global markets, taking into account the de facto effects of EU legislation and looking beyond territorial jurisdiction as a formal concept. (3) The extent to which third country laws and practices can influence EU behaviour in the digital domain, i.e., the reverse of the second element. According to Savin (2022), the extraterritorial application of EU legislation is a manifestation of EU's move towards increased digital sovereignty and Savin seems to conceptualize the 'Brussels effect' as a central aspect of the second criterion.

This aligns with the observation that there are various mechanisms enabling the EU to exercise its global regulatory influence, one of them being the 'Brussels effect' (Cervi, 2022). The term 'Brussels effect' connotes the EU's ability to extend power beyond its borders, alongside its ability to establish standards and require adherence to these in order to gain or maintain access to the European single market (Bradford, 2020; Bendiek & Stürzers, 2022). Following Bradford (2020), the 'Brussels effect' is underlined by five elements: market size, regulatory capacity, stringent standards, inelastic targets and non-divisibility.

A prominent example of the 'Brussels effect' is the GDPR. As such, it is tellingly to note that the GDPR is outlined as a data governance measure that strengthened digital sovereignty by putting *"individuals in control of their data"* and making the EU *"a standard-setter in privacy and data protection"* (Roberts et al., 2021 citing Madiega, 2020, p. 3). Finally, also Bendiek and Stürzer (2022) argue that the 'Brussels effect' can be leveraged to promote digital sovereignty.

Drawing on these considerations, this contribution operationalizes the likelihood that the CRA has a 'Brussels effect' as a strong indication that it adds to

cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ (2019) L 151/15 [hereinafter Cybersecurity Act].

the promotion of digital sovereignty. A ‘Brussels effect’ of the CRA seems to be at least the intention of the EU (Bertuzzi, 2022). Accordingly, this contribution is keen to evaluate whether the likelihood of a ‘Brussels effect’ of the CRA is present.

Although a conclusive answer to this question cannot be delivered in the scope of this extended abstract, certain assumptions may be made: If enacted, the CRA would allow the banning of products with digital elements that do not meet the requirements from the European market. Given that the CRA is likely to also apply to products from non-EU manufacturers once they are placed on the EU market, the CRA would impact cybersecurity standards for such products beyond the EU’s borders. Indeed, manufacturers of non-CRA-compliant products would not be able to participate in a large market, given that the European market is the third largest IoT adopter after the Asia-Pacific region and North America, and as the European IoT market is still growing (CBI, 2022). Moreover, considering, amongst others, that manufacturers must ensure that their digital products meet the essential CRA cybersecurity requirements at the outset and that GDPR-like fines can be imposed in case of non-compliance, the costs of maintaining a difference between EU-compliant and non-compliant products seem likely to be higher than the costs of merely implementing and adhering to the requirements set out by the CRA. Consequently, non-EU manufacturers may find it more convenient to follow the CRA’s rules as a standard for their global operations, instead of developing different products or processes for different markets, thereby fueling the Brussels effect and establishing the EU as a global standardsetter for the cybersecurity of connected devices, just as it already is in the area of data protection by means of the GDPR (Burri & Zihlmann, 2023; Saalman et al., 2022; Car & De Luca, 2022).

References

Banasiński, C. & Rojszczak, M. (2021): 'Cybersecurity of Consumer Products against the Background of the EU Model of Cyberspace Protection', *Journal of Cybersecurity*, 2021, pp. 1–15.

Barrinha, A. & Christou, G. (2022): 'Speaking Sovereignty: The EU in the Cyber Domain', *European Security*, 31(3), 2022, pp. 356–376.

Bellanova, R. & Carrapico, H. & Duez, D. (2022): 'Digital/sovereignty and European Security Integration: An Introduction', *European Security*, 31(3), 2022, pp. 337–355.

Bendiek, A. & Pander Maat, E. (2019): 'The EU's Regulatory Approach to Cybersecurity', German Institute for international and Security Affairs, WP NR. 02, 2019, retrieved 15 May 2023 from https://www.swpberlin.org/publications/products/arbeitspapiere/WP_Bendiek_Pander_Maat_EU_Approach_Cy bersecurity.pdf.

Bendiek, A. & Stürzer, I. (2022): 'Advancing European Internal and External Digital Sovereignty: The Brussels Effect and the EU-US Trade and Technology Council', German Institute for international and Security Affairs, SWP Comment 2022, retrieved 10 March 2023 from https://www.swpberlin.org/publications/products/comments/2022C20_EuropeanDigitalSovereignty.pdf.

Bertuzzi, L. (2023): 'Swedish Council Presidency Presents First Full Rewrite of Cyber Resilience Act', EURACTIV.com, 27 April 2023, retrieved 15 May 2023 from https://www.euractiv.com/section/cybersecurity/news/swedish-council-presidency-presentsfirst-full-rewrite-of-cyber-resilience-act/.

Bertuzzi, L. (2022): 'Commission Expects to Set the World's Cybersecurity Standards for Connected Devices', EURACTIV.com, 27 September 2022, retrieved 15 May 2023 from https://www.euractiv.com/section/cybersecurity/news/commission-expects-to-set-the-worldscybersecurity-standards-for-connected-devices/.

Bradford, A. (2020): The Brussels Effect: How the European Union Rules the World, Oxford 2020.

Breton, T. (2021): 'How a European Cyber Resilience Act Will Help Protect Europe', September 2021, retrieved 10 March 2023 from https://ec.europa.eu/commission/commissioners/20192024/breton/blog/how-european-cyber-resilience-act-will-help-protect-europe_en.

Broeders, D. & Cristiano, F. & Kaminska, M. (2023): 'In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions', *Journal of Common Market Studies*, 2023, pp. 1–20.

Burri, M. & Zihlmann, Z. (2023): 'The EU Cyber Resilience Act – An Appraisal and Contextualization', *Zeitschrift für Europarecht*, 2, 2023, pp. 1–45.

Car, P. & De Luca, S. (2022): 'EU Cyber-resilience Act', European Parliamentary Research Service, PE 739.259, December 2022.

Carr, M. & Lesniewska, F. (2020): 'Internet of Things, Cybersecurity and Governing Wicked Problems: Learning from Climate Change Governance', *International Relations*, 34(3), 2020, pp. 391–412.

CBI, Ministry of Foreign Affairs (2022): 'The European Market Potential for (Industrial) Internet of Things', 7 June 2022, retrieved 15 May 2023 from https://www.cbi.eu/marketinformation/outsourcing-itobpo/industrial-internet-things/market-potential.

Chiara, P. G. (2022): 'The Cyber Resilience Act: The EU Commission's Proposal for a Horizontal Regulation on Cybersecurity for Products with Digital Elements', *International Cybersecurity Law Review*, 3, 2022, pp. 255–272.

Commission Staff Working Document - Impact Assessment Report, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, Brussels, 15.9.2022, SWD(2022) 282 final, part 1/3, 1, (cit. Impact Assessment, 2022).

Committee on Industry, Research and Energy (2023): Draft Report on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, 31.3.2023, (COM(2022)0454 – C9-0308/2022 – 2022/0272(COD)), (cit. Draft Report, 2023).

Farrand, B. & Carrapico, H. (2022): 'Digital Sovereignty and Taking Back Control: From Regulatory Capitalism to Regulatory Mercantilism in EU Cybersecurity', *European Security*, 31(3), 2022, pp. 435–453.

Floridi, L. (2020): ‘The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU’, *Philosophy & Technology*, 33, 2020, pp. 369–378.
Gregersen, C.R. (2022): ‘EU Cyber Resilience Act: The GDPR for IoT’, embedded, 20 December 2022, retrieved 15 May 2023 from https://www.embedded.com/eu-cyber-resilience-act-thegdpr-for-iot/.
Kaloudis, M. (2022): ‘Sovereignty in the Digital Age – How Can We Measure Digital Sovereignty and Support the EU’s Action Plan?’, *New Global Studies*, 16(3), 2022, pp. 275–299.
Madiega, T. (2020): ‘Digital Sovereignty for Europe’, European Parliamentary Research Service, PE 651.992, July 2020.
Pohle, J. & Thiel, T. (2020): ‘Digital Sovereignty’, *Internet Policy Review*, 9, 2020, pp. 1–19.
Roberts, H. & Cowls, J. & Casolari, F. & Morley, J. & Taddeo, M. & Floridi, L. (2021): ‘Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies’, *Internet Policy Review*, 10, 2021, pp. 1–26.
Saalman, L. & Su, F. & Saveleva Dovgal, L. (2022): ‘Cyber Posture Trends in China, Russia, the United States and the European Union’, SIPRI, December 2022, retrieved 10 March 2023 from https://www.sipri.org/sites/default/files/2022-12/2212_cyber_postures_0.pdf.
Savin, A. (2022): ‘Digital Sovereignty and Its Impact on EU Policymaking’, Copenhagen Business School Law Research Paper Series No. 22-02, retrieved 10 March 2023 from https://ssrn.com/abstract=4075106.
Schmitz-Berndt, S. & Cole, M.D. (2022): ‘Towards an Efficient and Coherent Regulatory Framework on Cybersecurity in the EU: The Proposals for a NIS 2.0 Directive and a Cyber Resilience Act’, *Applied Cybersecurity & Internet Governance*, 1, 2022, pp. 1–17.
Soare, S.R. (2022): ‘How to Achieve Digital Sovereignty – A European Guide’ in D. Broeders (ed.): *EU Digital Sovereignty: From Narrative to Policy?*, EU Cyber Direct, December 2022, pp. 19–24.
von der Leyen, U. (2021): ‘2021 State of the Union Address by President von der Leyen’, September 2021, retrieved 10 March 2023 from https://ec.europa.eu/commission/presscorner/api/files/document/print/ov/speech_21_4701/SPEECH_21_4701_OV.pdf.
Weber, R. H. & Studer, E. (2016): ‘Cybersecurity in the Internet of Things: Legal Aspects’, *Computer Law & Security Review*, 32, 2016, pp. 715–728.
Zirnstein, Y. & Lee, Y. L. & Ge A. (2022): ‘Evolving Cybersecurity Landscape – Comparing the Regulatory Approaches in the EU, in China and in Singapore — An Analysis of Legislative Approaches to Key Issues in Tackling a Global Phenomenon’, *Computer Law Review International,* 6, 2022, pp. 165–172.

Session 2

Jasmijn Boeken(2022): Why Should I Care? A Caring Stakeholder Approach to Corporate Cybersecurity Strategy. In: EU Cybersecurity: Collective Resilience through Regulation, June 22nd 2023, Brussels - Belgium

Cybersecurity: Why Should I Care?

A Caring Stakeholder Approach to Corporate Cybersecurity Strategy

Jasmijn Boeken [a, b]
[a] Institute of Security and Global Affairs (ISGA), Leiden University
[b] Centre of Expertise Cyber Security, The Hague University of Applied Sciences
(j.boeken@fgga.leidenuniv.nl)

Introduction

Companies are currently dealing with the struggles of increased digitization: cyberattacks are constantly occurring (Ganin et al. 2020); no company, big or small, is safe (Buil-Gil et al. 2021); and at the bottom-line, cybercrime is costing society a considerable amount of money (Anderson et al. 2013). While companies are figuring out how to be secure in the digital domain, it remains a relatively new challenge that demands further research. The topic of this paper is cybersecurity within companies, as well as the business ethics that steers the behavior of these companies. Current corporate cybersecurity greatly emphasizes technical risk assessments (Schinagl and Shahim 2020). With a strong focus on being compliant rather than being secure, companies are striving to abide by the guidelines of cyber risk management models such as NIST and ISO but consequently suffer from blind spots (Groves 2009; Preston and Wickson 2016; Lundgren and Bergström 2019). Companies are in a mode of problem solving (Liedtka 1996), and focus on compliance to legal frameworks to stay on course. This paper will

connect companies' cybersecurity strategy with theories of business ethics to propose a new way of looking at cybersecurity strategy.

At the 50th World Economic Forum (WEF) meeting of 2020 in Davos, the stakeholder approach was described as a promising philosophy for organizations to cope with the new challenges of increased digitization (Mhlanga and Moloi 2020). This resulted in the Davos Manifesto 2020, setting ethical guidelines for companies on how to navigate these challenges, including a large focus on stakeholders (Schwab 2020). Likewise, at the Business Roundtable in that same year, 181 CEOs committed to leading their companies to the benefit of all stakeholders. In academia there is a similar rise in popularity of stakeholder theory (McVea and Freeman 2005).

For the other challenges of our time, for example climate change, ethical guidelines are developed, however, for cybersecurity this remains a gap (Morgan 2021). This paper fills this gap by applying business ethics to the domain of cybersecurity in companies. The research question that this paper will answer is: how can stakeholder theory guide companies in creating a cybersecurity strategy? This paper takes a philosophical approach and will by means of an integrative literature review (Snyder 2019) and conceptual analyses (Machado and Silva 2007) develop multiple lines of argumentation. It will compare the previously dominant shareholder theory to the upcoming stakeholder theory in the context of corporate cybersecurity to discover possible benefits of introducing stakeholder theory to this domain.

Shareholder Theory

Shareholder theory has long been the dominant paradigm within management science (Ghoshal 2005). According to this theory, the sole purpose of the firm is maximizing shareholders' profit (Margolis and Walsh 2003). This perspective was established in a landmark 1919 Michigan State Supreme Court decision on Henry Ford, stating that an organization's goal is to ensure profit for its shareholders (Margolis and Walsh 2003). In addition to its dominance in the academic discourse on business, in practice shareholder theory is often seen as the dominant paradigm for Western companies (Schwab 2019; Mhlanga and Moloi 2020). Most importantly, this view argues that companies do have the responsibility to abide to

the law, however, they are not responsible for anything that is beyond the letter of the law. In current corporate cybersecurity strategy, we can see this in the strong focus on compliance. While this is often the best a company can do, it has the danger of creating blind spots.

The pacing problem

In the case of corporate cybersecurity, this limitation to compliance introduces the pacing problem. It is commonly known that the pace of technological development is often much higher than the pace of development of laws. While this might bring the benefit of stability in certain cases, it also means less guidance for companies' cybersecurity. Marchant (2011) describes that the currently dominant ethical frameworks cannot keep up with the speed of technological developments. He contrasts this fast development of technology with the slow movements of government and calls this the "pacing problem". Consequently, we need a framework that can take companies' responsibility further than law. This paper suggests that the stakeholder approach might provide such a framework.

Stakeholder Theory

The 1984 seminal work of Freeman, *Strategic management: A stakeholder approach,* was written to provide corporations with a new way of approaching strategic management. His main argument is that corporations have more stakeholder groups than just the shareholders, and that these should be considered in companies' decision-making (Freeman 1984). The theory prescribes whom the firm should serve and how it should operate (Wicks et al. 1994). To organize the extensive research on the theory, Donaldson and Preston (1995) have divided it into descriptive, instrumental, and normative research. Whereas descriptive work deals with question of how companies currently do things (Greenley and Foxall 1996; Pedersen 2006); instrumental work studies the effects of stakeholder management on corporate goals like profit (Preston and Sapienza 1990; Waddock and Graves 1997; Orlitzky and Benjamin 2001; Ruf et al. 2001; Margolis and Walsh 2003; Orlitzky et al. 2003; Moon 2014); and normative work deals with the question of what a corporation ought to do (Wicks et al. 1994; Phillips 1997;

Freeman and Phillips 2002; Vos 2003; Freeman et al. 2010). This paper is situated in the normative domain of stakeholder theory, while not losing sights of the others because what is now normative theory might one day become the topic of a descriptive or instrumental research.

According to Freeman (1994), stakeholder theory should always be combined with a normative core, this will help determine who the relevant stakeholders are and what a firms' behavior should look like. Whether this normative core is based on Rawlsian theory (Phillips 1997), Kantian theory (Vos 2003), libertarian theory (Freeman and Phillips 2002), or ethics of care (Wicks et al. 1994), can vary. While the ethical cores all have some distinct benefits, what the first three have in common is that they propose some type of universal principles. For this paper, stakeholder theory will be used in combination with a normative core of ethics of care, which is divergent due to its ability to focus on specific context.

Care Ethics as the Normative Core

As described in the previous section, stakeholder theory requires a certain normative core. In this paper, that core will be Care Ethics. Having its roots in feminist theory, Gilligan's (1993) book *In a Different Voice,* became the leading work in care ethics. The five most generally mentioned features of care ethics are: (1) it sees care as a moral value, (2) it values emotions, (3) it considers context, (4) it reconceptualizes the public and private sphere, and (5) it has a relational conception of the person (Gilligan 1993; Held 2006; Preston and Wickson 2016). To give an example of how these principles can be translated to cybersecurity practices: care ethics entails that relationships should go beyond law (Hardwig 1984; Noddings 2013), merely complying and following a cyber risk management framework will not be enough. Furthermore, the effect of emotions on (security) behavior needs to be considered within the companies' cybersecurity strategy (Plot 2009; Kahneman 2011; Barrett 2017; Sapolsky 2017). The paper will further study the ways in which these caring principles can affect corporate cybersecurity strategy.

Talking about an obligation of care, Noddings (2013) identifies two criteria that need to be met for an obligation of care: (1) the existence or the potential existence of a relationship, and (2) the potential for growth within this relationship. Companies consist of webs of relationships, often including a

potential for growth, therefore, corporations might have the obligation to care for their stakeholders. The paper will study whether companies have an obligation of care regarding their cybersecurity, and how we can see investments in cybersecurity as an act of care for a companies' stakeholders.

Conclusion

The preliminary conclusion of this paper is that the suggestion of the WEF to introduce stakeholder theory as a way to manage cybersecurity has true potential. Especially in combination with the theory of ethics of care, introducing us with the obligation to care, a different view has been provided. The paper will, more extensively, argue why companies have the responsibility to care for their cybersecurity, and how this can be seen as an act of care for their stakeholders. The proposed importance of this research is twofold, one, it will change the way we look at cybersecurity in companies, and two, it will change the way we look at ethics in corporate governance. Taken together, this creates the possibility of guiding companies towards a caring cybersecurity strategy. What happens in academic literature can make an important impact on business ethics and thus influence the behavior of companies (Dobson and White 1995).

References

Anderson R, Barton C, Böhme R, et al (2013) Measuring the cost of cybercrime. In: The economics of information security and privacy. Springer, pp 265–300

Barrett LF (2017) How emotions are made: The secret life of the brain. Pan Macmillan

Buil-Gil D, Lord N, Barrett E (2021) The dynamics of business, cybersecurity and cyber-victimization: Foregrounding the internal guardian in prevention. Vict Offenders 16:286–315

Dobson J, White J (1995) Toward the feminine firm: An extension to Thomas White. Bus Ethics Q 463–478

Donaldson T, Preston LE (1995) The stakeholder theory of the corporation: Concepts, evidence, and implications. Acad Manage Rev 20:65–91

Freeman RE (1984) Strategic Management: A Stakeholder Approach. Cambridge University Press

Freeman RE (1994) The politics of stakeholder theory: Some future directions. Bus Ethics Q 409–421

Freeman RE, Harrison JS, Wicks AC, et al (2010) Stakeholder theory: The state of the art

Freeman RE, Phillips RA (2002) Stakeholder theory: A libertarian defense. Bus Ethics Q 12:331–349

Ganin AA, Quach P, Panwar M, et al (2020) Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. Risk Anal 40:183–199. https://doi.org/10.1111/risa.12891

Ghoshal S (2005) Bad management theories are destroying good management practices. Acad Manag Learn Educ 4:75–91

Gilligan C (1993) In a different voice: Psychological theory and women's development. Harvard University Press

Greenley GE, Foxall GR (1996) Consumer and nonconsumer stakeholder orientation in UK companies. J Bus Res 35:105–116

Groves C (2009) Future ethics: risk, care and non-reciprocal responsibility. J Glob Ethics 5:17–31

Hardwig J (1984) Should women think in terms of rights? Ethics 94:441–455

Held V (2006) The ethics of care: Personal, political, and global. Oxford University Press on Demand

Kahneman D (2011) Thinking, fast and slow. Macmillan

Liedtka JM (1996) Feminist morality and competitive reality: A role for an ethic of care? Bus Ethics Q 179–200

Lundgren M, Bergström E (2019) Security-related stress: A perspective on information security risk management. IEEE, pp 1–8

Machado A, Silva FJ (2007) Toward a richer view of the scientific method: The role of conceptual analysis. Am Psychol 62:671

Marchant GE (2011) Addressing the pacing problem. In: The Growing Gap between Emerging Technologies and Legal-Ethical Oversight. Springer, pp 199–205

Margolis JD, Walsh JP (2003) Misery loves companies: Rethinking social initiatives by business. Adm Sci Q 48:268–305

McVea JF, Freeman RE (2005) A names-and-faces approach to stakeholder management: How focusing on stakeholders as individuals can bring ethics and entrepreneurial strategy together. J Manag Inq 14:57–69

Mhlanga D, Moloi T (2020) The stakeholder theory in the fourth industrial revolution. Int J Econ Financ 12:352–368

Moon J (2014) Corporate social responsibility: A very short introduction. Oxford University Press, USA

Morgan G (2021) Ethical Issues in cybersecurity: employing red teams, responding to ransomware attacks and attempting botnet takedowns

Noddings N (2013) Caring: A relational approach to ethics and moral education. Univ of California Press

Orlitzky M, Benjamin JD (2001) Corporate social performance and firm risk: A meta-analytic review. Bus Soc 40:369–396

Orlitzky M, Schmidt FL, Rynes SL (2003) Corporate social and financial performance: A meta-analysis. Organ Stud 24:403–441

Pedersen ER (2006) Making corporate social responsibility (CSR) operable: How companies translate stakeholder dialogue into practice. Bus Soc Rev 111:137–163

Phillips RA (1997) Stakeholder theory and a principle of fairness. Bus Ethics Q 7:51–66

Plot FA (2009) Paying attention to attention: care and humanism. Soc Bus Rev

Preston CJ, Wickson F (2016) Broadening the lens for the governance of emerging technologies: Care ethics and agricultural biotechnology. Technol Soc 45:48–57

Preston LE, Sapienza HJ (1990) Stakeholder management and corporate performance. J Behav Econ 19:361–375

Ruf BM, Muralidhar K, Brown RM, et al (2001) An empirical investigation of the relationship between change in corporate social performance and financial performance: A stakeholder theory perspective. J Bus Ethics 32:143–156

Sapolsky RM (2017) Behave: The biology of humans at our best and worst. Penguin

Schinagl S, Shahim A (2020) What do we know about information security governance?"From the basement to the boardroom": towards digital security governance. Inf Comput Secur

Schwab K (2019) Why we need the "Davos Manifesto" for a better kind of capitalism. https://www.weforum.org/agenda/2019/12/why-we-need-the-davos-manifesto-for-better-kind-of-capitalism/#:~:text=By%20giving%20stakeholder%20capitalism%20concrete,United%20Nations%20Sustainable%20Development%20Agenda. Accessed 23 Jan 2023

Schwab K (2020) Davos Manifesto 2020: The Universal Purpose of a Company in the Fourth Industrial Revolution. https://www.weforum.org/agenda/2019/12/davos-manifesto-2020-the-universal-purpose-of-a-company-in-the-fourth-industrial-revolution/. Accessed 1 Oct 2023

Snyder H (2019) Literature review as a research methodology: An overview and guidelines. J Bus Res 104:333–339

Vos JF (2003) Corporate social responsibility and the identification of stakeholders. Corp Soc Responsib Environ Manag 10:141–152

Waddock SA, Graves SB (1997) The corporate social performance–financial performance link. Strateg Manag J 18:303–319

Wicks AC, Gilbert Jr DR, Freeman RE (1994) A feminist reinterpretation of the stakeholder concept. Bus Ethics Q 475–497

Parto Mirzaei (2022): The new F-word: The case of fragmentation in cybersecurity governance. In: EU Cybersecurity: Collective Resilience through Regulation, June 22nd 2023, Brussels - Belgium

The new F-word: The case of fragmentation in cybersecurity governance

Parto Mirzaei
Institute of Security and Global Affairs (ISGA), Leiden University, The Netherlands
Email address: p.mirzaei@fgga.leidenuniv.nl

Keywords: *EU cybersecurity, fragmentation, governance, institutional design, The Netherlands*

Abstract

Introduction

This paper concerns a case-study of the fragmentation of cybersecurity governance in the Netherlands. By mapping the different ministries and the way in which cybersecurity governance is conducted in the Netherlands, the paper demonstrates that there is evidence that there is currently a fragmented cybersecurity governance landscape in place. This research provides a foundation for future research to explore how fragmentation in cybersecurity governance operates on a granular level in the Dutch central government, and allows for the extrapolation to other countries in the European Union, and cybersecurity governance on an EU-level. Signs of fragmentation in (cyber)security governance and/or policy on a EU-level have already been discussed by several scholars (Carrapico & Barrinha, 2017; Christou, 2019; e Silva, 2013; Kasper, 2020). The EU has also stated that it recognises the complexity and the diversity of actors involved in the governance of cybersecurity in Europe, and has therefore argued that member states themselves should be responsible for preventing and responding to cyber-attacks and incidents (Christou, 2019). This paper allows

for an inward look in how one of the EU member states deals with cybersecurity governance on an individual member-state level.

The Dutch government identifies six national security interests for the Netherlands: territorial security; physical security; economic security; ecological security; social and political stability, and the international rule of law (NCTV, 2021; Silfversten et al., 2020). Cybersecurity is described as being an interlaced element in all of the above-mentioned fields of security interest (NCTV, 2021; Silfversten et al., 2020). The Dutch cybersecurity governance landscape is generally perceived as fragmented by politicians, policy makers and cybersecurity experts in both the public and the private sector in the Netherlands, as well as in academia (Cyber Security Raad, 2020a, 2020b, 2020c, 2021; GovCERT, 2011; KPMG, 2020; Ministerie van Binnenlandse Zaken, 2019, 2020a, 2020b; NCTV, 2022c; Rathenau Instituut, 2017; Schram et al., 2021; Timmers & Dezeure, 2020; Tweede Kamer, 2021, 2022). To date, no research has been conducted to investigate the accuracy of this perception with regards to Dutch cybersecurity governance. Yet, a decentralised governance approach is not novel; it has been a common approach for a variety of different topics such as environmental governance (Zuidema, 2017), energy infrastructure governance (Goldthau, 2014), and water governance (Dunn et al., 2014).

Recent research on governance fragmentation has tended to focus on international governance, climate, environmental, and artificial intelligence governance (Bakker & Cook, 2011; Cihon et al., 2020; Zelli, 2011; Zelli & van Asselt, 2013). Whilst fragmentation in governance may be part of a narrative of disadvantage, research has suggested it might also have beneficial features: for instance when it leads to the specialisation of distinct units (Smullen, 2004; Talbot, C, 2004).

Objective

Existing research on the governance of cybersecurity in the Netherlands has demonstrated that cybersecurity is currently vested with multiple ministries. The dominant ministries according to this research are: the Ministry of Justice and Security; the Ministry of the Interior and Kingdom Relations; the Ministry of Economic Affairs and Climate Policy; the Ministry of Defence; the Ministry of Infrastructure and Water Management, and the Ministry of Education, Culture and Science (Silfversten et al., 2020). When it comes to the protection

of critical infrastructure, the NCTV (the National Coordinator for Counterterrorism and Security) and the NCSC (National Cyber Security Centre) – which are both part of the Ministry of Justice and Security – have the task of protecting the Netherlands against threats that have the potential of disrupting society, through e.g. assuring the security of vital elements in Dutch society and economy (NCTV, 2022a). That cybersecurity governance is vested in several ministries and institutions – and allocated key structural funds – strongly suggests that cybersecurity is considered a primary issue of concern by the Dutch central government. Although there is a strong presumption that cybersecurity governance is indeed organised in a decentralised manner, the evidence for the fragmentation claims is somewhat meagre. Until now, the cybersecurity governance landscape of the Netherlands has not yet been mapped; therefore, claims of fragmentation are difficult to verify.

Method

To clarify whether the Dutch cybersecurity governance landscape is indeed fragmented, an inventory of the current actors and organisations within the central government has been made through open-source data on government websites and the study of policy documents in 2022 and 2023 on: tweedekamer.nl, overheid.nl, and rijksoverheid.nl, and other government organisations' websites. In the Netherlands, the central government has three core tasks: policy creation, implementation, and oversight (Rijksoverheid, n.d.-b). A distinction has been made between organisations that are concerned with cybersecurity governance *within* the central government, and organisations that are concerned with the creation, implementation, and/or oversight of cybersecurity policies towards Dutch society and Dutch citizens. The acquired data has subsequently been mapped and coded to determine the distinction between internal and external governance of cybersecurity, cybersecurity policy creation; implementation; and/or oversight.

The principal assessment criterion is that these organisations should be involved in cybersecurity governance, and this therefore only includes the organisations that operate on a strategic cybersecurity governance level. Besides the ministries, water authorities, municipalities, provinces, and security regions also have a(n) (in)formal responsibility in cybersecurity. These entities have been omitted from the scope of this research due to time and research constraints.

The primary object of analysis is the Dutch central government, and this paper focuses on the ways in which they manage cybersecurity governance vis-à-vis Dutch society and Dutch citizens.

Findings

The Dutch central government consists of twelve ministries (Rijksoverheid, n.d.-a). Firstly, All the ministries and organisation of the Dutch central government have been mapped and coded in an Excel overview, based on open-source information on organizations and ministries and organisational government websites in 2022-2023. The steps and considerations mentioned in the methodology section have ultimately led to an overview of 35 organisations within seven ministries that are concerned with cybersecurity governance in the Netherlands (see Table I).

Argument

Thus far, it can be concluded that the governance of cybersecurity in the Netherlands has indeed developed in a fragmented manner. The relevance of this research lies in the fact that this fragmented institutional cybersecurity governance design could potentially impact the creation, implementation, and oversight of cybersecurity policies. This paper could therefore serve as a foundation for further research into the implications of fragmentation in cybersecurity governance at a Member State level and allows us to understand more about whether and how this phenomenon impacts the resilience of cybersecurity in the EU.

References

Bakker, K., & Cook, C. (2011). Water Governance in Canada: Innovation and Fragmentation. *International Journal of Water Resources Development*, *27*(2), 275–289. https://doi.org/10.1080/07900627.2011.564969

Carrapico, H., & Barrinha, A. (2017). The EU as a Coherent (Cyber)Security Actor?: The EU as a Coherent (Cyber)Security Actor? *JCMS: Journal of Common Market Studies*, *55*(6), 1254–1272. https://doi.org/10.1111/jcms.12575

Christou, G. (2019). The collective securitisation of cyberspace in the European Union. *West European Politics*, *42*(2), 278–301. https://doi.org/10.1080/01402382.2018.1510195

Cihon, P., Maas, M. M., & Kemp, L. (2020). Fragmentation and the Future: Investigating Architectures for International AI Governance. *Global Policy*, *11*(5), 545–556. https://doi.org/10.1111/1758-5899.12890

Cyber Security Raad. (2020a). *CSR Jaaroverzicht 2019* (pp. 1–13). https://www.cybersecurityraad.nl/documenten/verslagen/2020/04/01/csr-jaaroverzicht-2019

Cyber Security Raad. (2020b). *CSR Werkprogramma 2020-2021*. https://www.cybersecurityraad.nl/overige-publicaties/documenten/jaarplannen/2020/07/01/csr-werkprogramma-2020-2021

Cyber Security Raad. (2020c). *CSR Urgentieverklaring*. https://www.cybersecurityraad.nl/documenten/adviezen/2020/03/31/csr-urgentieverklaring

Cyber Security Raad. (2021). *CSR Adviesrapport: Integrale aanpak cyberweerbaarheid* (pp. 3–72). Cyber Security Raad. https://www.cybersecurityraad.nl/documenten/adviezen/2021/04/06/csr-adviesrapport-integrale-aanpak-cyberweerbaarheid

Dunn, G., Bakker, K., & Harris, L. (2014). Drinking Water Quality Guidelines across Canadian Provinces and Territories: Jurisdictional Variation in the Context of Decentralized Water Governance. *International Journal of Environmental Research and Public Health*, *11*(5), 4634–4651. https://doi.org/10.3390/ijerph110504634

e Silva, K. (2013). Europe's fragmented approach towards cyber security. *Internet Policy Review*, *2*(4). https://doi.org/10.14763/2013.4.202

Goldthau, A. (2014). Rethinking the governance of energy infrastructure: Scale, decentralization and polycentrism. *Energy Research & Social Science*, *1*, 134–140. https://doi.org/10.1016/j.erss.2014.02.009

GovCERT. (2011). *Cybersecuritybeeld Nederland December 2011* (pp. 1–60). https://www.tweedekamer.nl/kamerstukken/detail?id=2011D64639&did=2011D64639

Kasper, A. (2020). The future of the European Union: Demisting the Debate. In *EU cybersecurity governance – stakeholders and normative intentions towards integration* (pp. 166–185). https://www.um.edu.mt/library/oar/handle/123456789/52308

KPMG. (2020). *SWOT-analyse strategische waardeketens*. https://www.rijksoverheid.nl/documenten/rapporten/2020/10/30/swot-analyse-strategische-waardeketens

Ministerie van Binnenlandse Zaken. (2019). *Conceptverslag Openbare kennisbijeenkomst—Tijdelijke Commissie Digitale Zaken* (pp. 1–84). https://www.tweedekamer.nl/kamerstukken/commissieverslagen/detail?id=2019D39722&did=2019D39722

Ministerie van Binnenlandse Zaken. (2020a). *Parlementair onderzoek digitale toekomst* (pp. 1–45). https://www.tweedekamer.nl/kamerstukken/detail?id=2020Z09430&did=2020D20305

Ministerie van Binnenlandse Zaken. (2020b). *Meer parlementaire grip op digitalisering* (pp. 1–16). https://www.tweedekamer.nl/kamerstukken/detail?id=2021D00178&did=2021D00178

NCTV. (2021). *Cybersecuritybeeld Nederland*. https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021

NCTV. (2022a). *Organisatie*. NCTV. https://www.nctv.nl/organisatie

NCTV. (2022b). *Nederlandse Cybersecuritystrategie 2022-2028*. https://www.ncsc.nl/onderwerpen/nederlandse-cybersecurity-strategie

Rathenau Instituut. (2017). *Opwaarderen Borgen van publieke waarden in de digitale samenleving* (pp. 1–213). https://www.tweedekamer.nl/kamerstukken/detail?id=2017D04400&did=2017D04400

Rijksoverheid. (n.d.-a). *Organisatie Rijksoverheid*. Rijksoverheid. https://www.rijksoverheid.nl/onderwerpen/rijksoverheid/organisatie-rijksoverheid

Rijksoverheid. (n.d.-b). *Taken van de Rijksoverheid*. https://www.rijksoverheid.nl/onderwerpen/rijksoverheid/taken-van-de-rijksoverheid

Schram, J., den Uijl, H., & van Twist, M. (2021). *Actuele kwestie, klassieke afweging*. Nederlandse School voor Openbaar Bestuur (NSOB). https://www.nsob.nl/over-nsob/actualiteiten/nieuwe-publicatie-actuele-kwestie-klassieke-afweging

Silfversten, E., Jordan, V., Martin, K., Dascalu, D., & Frinking, E. (2020). *Cybersecurity A State-of-the-art Review: Phase 2*. WODC. https://repository.wodc.nl/bitstream/handle/20.500.12832/3016/3051-cybersecurity-a-state-of-the-art-review-full-text.pdf?sequence=13&isAllowed=y

Smullen, A. (2004). Lost in translation? Shifting interpretations of the concept of ‘agency’: The Dutch case. In *Unbundled government: A Critical Analysis of the Global Trend to Agencies, Quangos and Contractualisation* (pp. 184–202). Routledge.

Talbot, C. (2004). The Agency Idea: Sometimes old, sometimes new, sometimes borrowed, sometimes untrue. In *Unbundled government: A Critical Analysis of the Global Trend to Agencies, Quangos and Contractualisation.* (pp. 3–21). Routledge.

Timmers, P., & Dezeure, F. (2020). *Nederlandse strategische autonomie en cybersecurity* (pp. 1–72). https://www.cybersecurityraad.nl/documenten/rapporten/2021/02/18/onderzoeksrapport-digitale-autonomie

Tweede Kamer. (2021). *Regels ter uitvoering van Verordening (EU) 2019/881 (Uitvoeringswet cyberbeveiligingsverordening)* (pp. 1–10). https://www.tweedekamer.nl/kamerstukken/detail?id=2021Z08205&did=2021D23776

Tweede Kamer. (2022). *Debat op hoofdlijnen over digitale zaken (ongecorrigeerd stenogram)*. Tweede Kamer Der Staten-Generaal. https://www.tweedekamer.nl/kamerstukken/detail?id=2022D28327&did=2022D28327

Zelli, F. (2011). The fragmentation of the global climate governance architecture. *WIREs Climate Change*, *2*(2), 255–270. https://doi.org/10.1002/wcc.104

Zelli, F., & van Asselt, H. (2013). Introduction: The Institutional Fragmentation of Global Environmental Governance: Causes, Consequences, and Responses. *Global Environmental Politics*, *13*(3), 1–13. https://doi.org/10.1162/GLEP_a_00180

Zuidema, C. (2017). *Decentralization in environmental governance: A post-contingency approach*. Routledge.

Tables

Table I: Overview of ministries and public organisations that are concerned with cybersecurity governance.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	Ministerie van Buitenlandse Zaken	Ministerie van Justitie en Veiligheid	Ministerie van Defensie	Ministerie van Economische Zaken en Klimaat	Ministerie van Financiën	Ministerie van Infrastructuur en Water

Logius	Directie Veiligheidsbeleid	NCTV	DCSC	Rijksinspectie Digitale Infrastructuur	De Nederlandsche Bank	Autoriteit Nucleaire Veiligheid en Stralingsbescherming
Forum Standaardisatie	Crisis Coördinator	NCSC	Defensie Cyber Commando	DICTU	Belastingdienst: Team Security, Continuity & Privacy	Rijkswaterstaat
Chief Information Office		ISACS	Koninklijke Marechaussee	Dcypher	Belastingdienst: Fiscale Inlichtingen- en opsporingsdienst	
CIO-Rijk		MCCb	MIVD	Digital Trust Center		
SSC ICT		ICCb				
AIVD		NKC				
NBV		Openbaar Ministerie				
Adviescollege ICT-toetsing		Autoriteit Persoonsgegevens				
Rijksbeveiligingsambtenaar		Politie				
CERT/CSIRT						
Rijksdienst voor Identiteitsgegevens						

Legend:
Red = internal governance
Green = policy creation
Purple = policy implementation
Blue = policy oversight

Yuliya Miadzvetskaya (2022): EU sanctions in response to cyber-attacks: punitive or preventive measures? In: EU Cybersecurity: Collective Resilience through Regulation, June 22nd 2023, Brussels – Belgium

EU sanctions in response to cyber-attacks: punitive or preventive measures?

Yuliya Miadzvetskaya
University of Tuebingen
yuliya.miadzvetskaya@coleurope.eu

Abstract

While EU restrictive measures are meant to be preventive in nature, horizontal sanctions frameworks resemble punitive measures adopted in response to a specific type of misbehavior. Can those horizontal sanctions be compared to a form of personalized punitive measures? Do they act as a substitute when a criminal persecution cannot take place or a suspect is out of reach for EU authorities (e.g. Russian hackers)? Or do they act as 'name and shame' instruments when the attribution of responsibility by the EU to a third State is not possible (e.g. cyberattacks)?

By using sanctions in response to cyber-attacks as a case study, this article identifies some elements that confirm the steadily growing punitive nature of thematic sanctions, notably the triggering situation posing threat to the EU itself (e.g. cyber-attacks), the way how reasons for listing are being crafted, the time frame of a sanctioned act. Despite the growing tendency toward the use of sanctions as punitive measures, there are few arguments against the open recognition of their punitive character.

1. Introduction

The growing personification of restrictive measures raises questions as to whether sanctions are comparable to law enforcement measures or to a form of individual punishment. The EU institutions and the European Court of Justice (ECJ) traditionally refer to sanctions as preventive measures that are not meant to be punitive. Nevertheless, this rigid view on sanctions enshrined in EU official documents[1] and the case-law[2] contrasts with a more daring assessment of sanctions by political scientists. The latter describe sanctions as "penalties linked to real or alleged misconduct"[3] and admit that "the desire to punish will always be an integral factor" in the imposition of sanctions.[4] Some legal scientists are also of the opinion that the punitive nature of sanctions must be acknowledged.[5]

This contribution seeks to explore the growing confusion between the preventive and punitive nature of EU sanctions by analyzing the specific case of sanctions in response to cyber-attacks. They constitute a novel sanctions regime that lays down foundations of personalized deterrence with respect to malicious cyber actors. The choice of this specific case study resides in the fact that a computer crime is recognized as crime under Article 83(1) TFEU. Consequently, sanctions adopted under the Common Foreign and Security Policy (CFSP) act as substitute measures or complementary measures to criminal penalties that are foreseen for the same type of activities under the EU and national laws. In that sense, targeted thematic sanctions represent a form of personalized punishment outside the scope of usually burdensome criminal proceedings.

The increasing personification of EU sanctions logically led to their decoupling from a specific State. Since late 90s, following the U-turn in the sanctions practice at the UN level, the EU started using targeted restrictive measures.[6] The EU pursued the objective of targeting only those responsible for a misconduct and hitting the least possible the broad population of the country. The emergence of a series of new EU autonomous horizontal sanctions regimes since 2018[7] was well embedded in this "Zeitgeist" of the EU sanctions policy. Notably it further reconfirmed their targeted nature by limiting potential negative humanitarian consequences, decoupled sanctions from a specific country listing, brought more flexibility into the EU sanctions practice and decreased the politization of restrictive measures.

Horizontal sanctions frameworks marked a new period in the EU sanctions practice by linking sanctions to a specific type of misbehavior, making them more precise in their formulation,

---

[1] Council of the European Union, Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy 5664/18 (2018), para 45.

[2] Case Sison v Conseil, T-47/03 ECLI:EU:T:2007:207 (2007) para 101: "The allegation that the Council has arrogated to itself a judicial role and powers in criminal matters not envisaged by the Treaty must be rejected. It is after all based on the mistaken premiss that the restrictive measures at issue in this case are of a criminal nature." Cases C-584/10 P, C-593/10 P and C-595/10 P", Commission and United Kingdom v Kadi ECLI:EU:C:2013:518 (2013) para 130 (Kadi II).

[3] Kim Richard Nossal, 'International Sanctions as International Punishment' (1989) 43(2) International Organization 301.

[4] Margaret P Doxey, International Sanctions in Contemporary Perspective (Macmillan 1987) 4.

[5] Nienke van der Have, 'The Proposed EU Human Rights Sanctions Regime – A First Appreciation' (2019) 30 Security and Human Rights 56, 71.

[6] Clara Portela, 'Are European Union Sanctions "Targeted"?' (2016) 29(3) Cambridge Review of International Affairs 912; UN Security Council Resolution 661 (1991); Francesco Giumelli, 'Understanding United Nations Targeted Sanctions: An Empirical Analysis' (2015) 91(6) International Affairs 1351.

[7] The 2001 EU terrorist list has UN origins and was enacted following the 11th September attacks.

notably listing criteria and reasons for listing. At the moment, the EU has 4 horizontal sanctions regimes in place: EU terrorist list,[8] sanctions in response to the use of chemical weapons,[9] sanctions in response to cyber-attacks[10] and gross human rights violations.[11] EU restrictive measures in response to disinformation campaigns are under discussions. The European Parliament has been actively calling for their enactment.[12] Sanctions in response to the use of chemical weapons[13] is the first full-fledged autonomous EU horizontal sanctions framework that to a large extent was mirrored in the subsequent horizontal sanctions frameworks (e.g. cyber-attacks and gross human rights violations).

Are those horizontal sanctions comparable to criminal sanctions? Do they act as a substitute when a criminal persecution cannot take place or a suspect is out of reach of EU authorities (e.g. Russian hackers)? This contribution reflects on the potential punitive or criminal nature of EU restrictive measures adopted under the horizontal sanctions frameworks. The reflection on the administrative or criminal nature of EU sanctions is important amidst the current debates on the potential confiscation of frozen assets or the criminalization of sanctions violations.

The paper is structured as follows. First, it explores the evolution of EU sanctions implying their growing personification that makes them sometimes resemble law enforcement measures. Such personification is rooted in the shift from broad country specific measures to individual thematic sanctions. Then, drawing on the existing case-law and scholarship, it reflects whether EU horizontal sanctions are preventive or punitive measures. The book chapter argues that while restrictive measures in response to cyber-attacks present certain similarities with criminal sanctions, there is a number of arguments against this qualification. EU sanctions in response to cyber-attacks are preventive measures by their nature but punitive in their effects since they can act as crime prevention measures or "quasi-countermeasures" to respond to any deviation from national, European and international cyber rules and norms.

2. From country specific to thematic individual sanctions

[8] Council Decision (CFSP) 2016/1693 concerning restrictive measures against ISIL (Da'esh) and Al-Qaeda and persons, groups, undertakings and entities associated with them and repealing Common Position 2002/402/CFSP OJ L 255/25 (2016); Council Regulation (EU) 2016/1686 of 20 September 2016 imposing additional restrictive measures directed against ISIL (Da'esh) and Al-Qaeda and natural and legal persons, entities or bodies associated with them OJ L 255/1 (2016); Council Common Position on the application of specific measures to combat terrorism OJ L 344/93 (2001); Council Regulation (EC) 2580/2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism OJ L 344/71 (2001).

[9] Council Decision (CFSP) 2018/1544 concerning restrictive measures against the proliferation and use of chemical weapons [2018] OJ L259/25; Council Regulation (EU) 2018/542 concerning restrictive measures against the proliferation and use of chemical weapons [2018] OJ L259/12.

[10] Council Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States [2019] OJ L129/13; Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States [2019] OJ L129/1.

[11] Council Decision 2020/1999 concerning restrictive measures against serious human rights violations and abuses (2020) OJ L410/13; Council Regulation (EU) 2020/1998 concerning restrictive measures against serious human rights violations and abuses (2020) OJ L410/1.

[12] See European Parliament, Draft Report of 18 October 2021 on foreign interference in all democratic processes in the European Union, including disinformation (2020/2268(INI)); European Parliament Press Release, 'EU should build a sanctions regime against disinformation' (25 January 2022) available at https://www.europarl.europa.eu/news/en/press-room/20220119IPR21313/eu-should-build-a-sanctions-regime-against-disinformation

[13] Council Decision (CFSP) 2018/1544 concerning restrictive measures against the proliferation and use of chemical weapons [2018] OJ L259/25; Council Regulation (EU) 2018/542 concerning restrictive measures against the proliferation and use of chemical weapons [2018] OJ L259/12.

This section will shed light on the increasing personification of EU restrictive measures and the evolution of the corresponding legal bases. This trend was, however, considerably impacted by the Russian war in Ukraine that triggered a substantial reconsideration of the EU sanctions practice. It would not be an exaggeration to say that the EU went through a 'mini revolution' and shifted from targeted to broad economic measures.

Up until the year 2021, that was marked by unprecedented sanctions first against Belarus[14] and then both Belarus and Russia in 2022, the EU was using targeted restrictive measures, including via thematic individual sanctions. The trend to adopt targeted sanctions emerged in mid-90s when the UN and then the EU for humanitarian considerations shifted from broad economic measures to so-called smart sanctions.[15] This change, however, was not reflected in the EU primary law. The wording of the EU Treaties back then did not provide for a specific competence for the adoption of sanctions against individuals.[16] Both Articles 301 and 60 EC (predecessors of Article 75 and 215 TFEU) explicitly referred to "third countries" and were silent on private persons. Such omission of individuals is understandable given that sanctions were previously used against third countries and consisted of economic measures.[17] Despite the absence of a specific legal basis for the enactment of individual sanctions, the Council interpreted those provisions broadly and adopted targeted restrictive measures against natural persons.[18]

The Court of Justice, in turn, clarified the confusing wording of Treaty provisions (Articles 60 EC and 301 EC) and confirmed that sanctions with respect to third countries shall be interpreted as including "the rulers of such a country and also individuals and entities associated with or controlled, directly or indirectly, by them".[19] Later on, the Treaty of Lisbon provided a firmer legal basis for restrictive measures targeted at individuals. Now Article 215 TFEU sets out an explicit competence for sanctions "against natural or legal persons and groups or non-State entities."

In 2018 the EU went further in its policy of sanctions personification and decoupled some sanctions from country related listings. The shift from country focused sanctions to sanctions targeting a specific misconduct required the adoption of respective legal frameworks. The EU introduced thematic sanctions on the use of chemical weapons,[20] followed by similar

[14] In response to the Ryanair plane incident, the EU introduced a flight ban and sectoral economic sanctions against Belarus.

[15] Clara Portela, 'Are European Union Sanctions "Targeted"?' (2016) 29(3) Cambridge Review of International Affairs 912; UN Security Council Resolution 661 (1991); Boutros Boutros-Ghali, 'Supplement to An Agenda for Peace: Position Paper of the Secretary General on the Occasion of the Fiftieth Anniversary of the United Nations' (1995) UN Doc. A/50/60-S/95/1, para 70.

[16] Peter Van Elsuwege, 'The Adoption of "Targeted Sanctions" and the Potential for Inter-Institutional Litigation after Lisbon', Journal of Contemporary European Research 7, no. 4 (19 December 2011): 488–99.

[17] For instance, the coordinated action in the form of economic sanctions by the European Political Cooperation (EPC) following the occupation of the US Embassy in Teheran in 1980; Regulation (EEC) 596/82 laying down economic sanctions against the Soviet Union (again in the absence of a UN Security Council resolution) following the imposition of martial law in Poland (1982) OJ L72/15; Regulation (EEC) 877/82 on economic sanctions against Argentina following the invasion of the Falkland Islands (1982) OJ L102/1. See M. Cremona, "EC Competence, 'Smart Sanctions' and the Kadi Case", Yearbook of European Law (2009), 559-592.

[18] Common Position of 19 March 1998 on restrictive measures against the Federal Republic of Yugoslavia, OJ (1998) L 95/1 and Common Position of 7 May 1998 concerning the freezing of funds held abroad by the Federal Republic of Yugoslavia (FRY) and Serbian Governments, OJ (1998) L 143/1.

[19] Joined Cases C-402/05 P and C-415/05 P Kadi & Al Barakaat ECLI:EU:C:2008:461 (2008), paras 166 and 168.

[20] Council Decision (CFSP) 2018/1544 cit.; Council Regulation (EU) 2018/542 cit.

frameworks on cyber-attacks[21] and gross human rights violations.[22] Those thematic sanctions are not the first autonomous measures of this kind introduced by the EU with the counter-terrorism related sanctions being the first example thereof.[23] The introduction of horizontal sanctions frameworks is a clear manifestation of a broader tendency to make sanctions as targeted as possible.

The EU sanctions in response to cyber-attacks were brought into existence through a standard two-step procedure. First, the Council CFSP Decision (CFSP), adopted on the basis of Article 29 TEU, lays down the overall sanctions framework. Second, it is implemented by the associated Regulation, adopted on the basis of Article 215 TFEU. The main attributes of EU sanctions in response to cyber-attacks is their global scope. Natural and legal persons are included on sanctions lists independently of their links with a specific country. This feature differentiates thematic sanctions from any other sanctions frameworks that are taken in response to security or democracy related situation in a third State. Similarly to other sanctions, thematic sanctions are not meant to last forever and are subject to review every year.

Sanctions in response to cyber-attacks fall under the category of smart, unilateral and autonomous sanctions. 'Smart' in the sense that they target individuals and entities involved in specific malicious activities and do not produce negative effects on the population of the target state. Even more so, thematic sanctions are meant to decouple sanctions from power structures of the State. Those measures include travel bans, asset freezes and prohibitions to make funds and economic resources available. They qualify as autonomous sanctions since they are enacted by the EU independently from the UN Security Council. The autonomy does not exclude cooperation with like-minded partners that share similar values and approaches to responsible State behaviour in cyberspace.[24]

3. Individual thematic sanctions: Punitive or preventive measures?

The growing personification of restrictive measures raises questions as to the blurring between sanctions as administrative and as criminal measures. Some scholars questioned whether asset freezes could be comparable to criminal sanctions,[25] others put into doubt the preventive nature of sanctions given their unlimited duration.[26] Nanopoulos pointed out to the blurring between sanctions as tools of warfare and law enforcement.[27] Nienke van der Have has called for the recognition of the punitive aspect of individual sanctions.[28] And more generally some scholars proposed to refer to the CFSP as a punitive policy given that 70

[21] Council Decision (CFSP) 2019/797 cit.; Council Regulation (EU) 2019/796 cit.

[22] Council Decision 2020/1999, cit., and Council Regulation (EU) 2020/1998, cit.

[23] The first EU terrorist lists had UN origins and were enacted following the 11th September attacks, see Common Position 2001/931/CFSP, (2001) OJ L 344/93; Council Regulation EC/2580/2001 (2001) OJ L 344/70 implementing UN Security Council Resolution 1373 (2001); EC Regulation 881/2002, (2003) OJ L 139/9, 29.5.2002, implementing UN Security Council Resolution 1267 (1999), of 15 Oct. 1999.

[24] For more on discussions between like-minded States on the application of international law to cyberspace see François Delerue, 'Cyber Operations and International Law' (Cambridge University Press, 2020), 14-24.

[25] Nienke van der Have, 'The Proposed EU Human Rights Sanctions Regime – A First Appreciation' cit.

[26] Christina Eckes, 'EU Restrictive Measures against Natural and Legal Persons: From Counterterrorist to Third Country Sanctions', 51(3) Common Market Law Review (2014).

[27] Eva Nanopoulos, The Juridification of Individual Sanctions and the Politics of EU Law (Bloomsbury Publishing, 2020).

[28] Nienke van der Have, 'The Proposed EU Human Rights Sanctions Regime – A First Appreciation' cit.

percent of decisions adopted under the CFSP are related to sanctions.[29] Together with my co-author Challet we also argued that sanctions are no longer preventive but rather punitive measures.[30]

The growing personification of restrictive measures raises questions as to whether sanctions are comparable to law enforcement measures or to a form of individual punishment. The debate on whether EU sanctions amount to punitive or criminal measures also gets traction given the contemplated changes in the EU sanctions practice, notably the potential confiscation of frozen assets and qualification of sanctions evasions as a crime under Article 81(3) TFEU. The EU legislators seem to look for any possible legal anchor justifying the seizure of Russian assets. This section will explore where resides the difference between preventive and punitive measures. On the basis of the analysis of sanctions in response to cyberattacks this section will reflect on whether thematic sanctions present certain similarities with criminal measures.

3.1. Difference between punitive and preventive measures

This section will examine the difference between punitive and preventive measures. One route for answering this question is to look at whether the measure in question stems from the field of criminal or administrative law. The delimitation between criminal and administrative measures in EU Law is not straightforward.[31] The EU administrative law develops at a high pace. Consequently, there is an increasing number of administrative sanctions, e.g. in the field of competition law, data protection law and financial regulations that present many similarities with criminal sanctions. The artificial de-criminalisation of certain behaviours in order to avoid a more stringent procedural requirements under criminal law can bear negative consequences for individuals and their fundamental rights. And the case of EU restrictive measures is no exception to this.

The term sanction that is commonly used to name EU restrictive measures is somehow misleading since sanction normally refers to a final stage of the criminal proceeding. EU restrictive measures, in contrast, are conceived as administrative measures with a preventive purpose. Preventive in nature, restrictive measures can have punitive effects.[32] This punitive component raises questions as to their resemblance to criminal law rules.

The term ‘criminal’ usually refers to sanctions of a severe nature that are intended to punish rather than simply deter in contrast to civil or administrative sanctions.[33] Criminal sanctions differ from administrative measures from the point of view of procedure since they entail an establishment of guilt and a higher standard of proof, notably a proof of past conduct beyond

---

[29] Ramses A Wessel, Elias Anttila, Helena Obenheimer and Alexandru Ursu, ‘The Future of EU Foreign, Security and Defence Policy: Assessing Legal Options for Improvement’ (2021) 26(5–6) European Law Journal 375.

[30] Yuliya Miadzvetskaya, Celia Challet. Are EU restrictive measures really targeted, temporary and preventive? The case of Belarus. Eur. World. Vol. 6(1).

[31] J. Vervaele, The Europeanisation of Criminal Law and the Criminal Law Dimension of European Integration. Research Papers in Law 3/2005, 10.

[32] Francesca Galli, The freezing of terrorists’ assets: preventive purposes with a punitive effect in Francesca Galli, Anne Weyembergh (eds.) Do Label Still Matter? Blurring boundaries between administrative and criminal law. The influence of the EU (Bruxelles, 2014).

[33] Jacob Öberg, ‘The Definition of Criminal Sanctions in the EU’, European Criminal Law Review 3 (2014): 273–99, https://doi.org/10.5235/219174414809354837.

reasonable doubt.[34] The administrative measures offer a rather quick solution to a problem in contrast to the criminal law that implies a lengthy cumbersome process.

The difference in procedures between criminal law measures and sanctions is rather straightforward. The European Court of Human Rights defined a criminal charge as "the official notification given to an individual by the competent authority of an allegation that he has committed a criminal offence".[35] Sanctions under the CFSP do not foresee any prior notification to listed individuals before sanctions are imposed on them.[36] It is a general rule that the statement of reasons is notified to the person concerned at the same time as the act affecting them comes into force.[37] This is due to the fact that prior disclosure of restrictive measures would jeopardize their surprise effect.[38] However, these considerations are not valid in the context of subsequent acts updating previous sanctions frameworks. In this case, notification obligations are compulsory if the Council relies on updated reasons for listing.[39]

Sanctioned individuals can exercise their defense rights and challenge EU restrictive measures on ex-post basis, in other words after someone has been listed. While the European Courts have considerably improved their standard of review and procedures in sanctions related litigations,[40] they are not comparable to criminal trials. In the US, for instance, courts provide for an exceptionally low standard of review for sanctions related cases.[41]

The Strasbourg Court singled out three criteria, that are also relied upon by the European Court of Justice,[42] in order to determine whether a measures qualifies as a criminal or administrative charge. They are better known as the "Engel Test".[43] First criteria is to know whether the provision(s) defining the offence belongs to criminal law according to domestic law. The second and third criteria are about the very nature of the offence and the severity of the sanction and its interference with fundamental rights of individuals affected. The following sections will examine EU sanctions in response to cyber-attacks specifically and sanctions more broadly on their fulfilment of some criteria of the "Engle Test" to qualify as criminal.

3.2. EU classification: restrictive measures are exclusively preventive

---

[34] Petter Asp, 'Blacklisting Sanctions and Principles of Criminal Law' in EU Sanctions: Law and Policy Issues Concerning Restrictive Measures, (I. Cameron, ed.) (Intersentia, 2013), 133.

[35] Deweer v. Belgium EctHR, Appl. no. 6903/75 (1980) para 42, 46; Eckle v. Germany ECtHR Appl. no. 8130/78 (1982) para 73.

[36] Melissa van den Broek, Monique Hazelhorst, and Wouter de Zanger, 'Asset Freezing: Smart Sanction or Criminal Charge?', Utrecht Journal of International and European Law 27, no. 2 (2010): 18–27, 26. Joined Cases C-402/05 P and C-415/05 P Kadi and Al Barakaat International Foundation v Council and Commission (2008) ECLI:EU:C:2008:461, para 338.

[37] T-307/12 and T-408/13 Mayaleh v Council ECLI:EU:T:2014:926 (2014) para 85.

[38] Joined Cases C-402/05 P and C-415/05 P Kadi and Al Barakaat International Foundation v Council and Commission, para 340.

[39] Case T-765/15 BelTechExport v Council ECLI:EU:T:2017:669, paras 116-122.

[40] Vigjilenca Abazi and Christina Eckes, "Closed Evidence in EU Courts: Security, Secrets and Access to Justice," 55(3), Common Market Law Review (2018).

[41] In 2012, the US District Court of Columbia applied an exceptionally low standard of review when reviewing Kadi's listing limited its review to the question of whether the agency's decision was "arbitrary and capricious".

[42] Case C-105/03 Mario Pupino ECLI:EU:C:2005:386 (2006).

[43] ECtHR, Engel and Others v. the Netherlands, App. nos. 5100/71, 5101/71, 5102/71, 5354/72, 5370/72 (1976) paras. 82-83.

This section will look at whether sanctions could be qualified as criminal measures on the basis of the Engel test. The first criteria relates to the qualification of the provision that defines an offence as criminal. Sanctions in response to cyberattacks are imposed to address serious cases of information system interference that would qualify as a crime under Article 83(1) and would constitute a crime under the EU Cybercrime Directive and national rules that implement it at Member States level.

Nevertheless, despite the recognition of a computer crime as a crime that could be punished with imprisonment and fines, sanctions under the Common Foreign and Security Policy constitute a different type of instruments. They are foreign policy measures enacted on the basis of Article 29 TEU and 215 TFEU by the EU for ensuring the State responsible behaviour in cyberspace and serve as a cyber deterrence instrument. The enactment of restrictive measures on the basis of proposals made by the Member States and the High Representative of the Union for Foreign Affairs and Security Policy (HR/VP) reconfirms their administrative nature. The nature of procedures for the composition of EU sanctions listings rules out their potential equation to criminal penalties.

According to the 2018 Council guidelines, sanctions are preventive and are not meant to be punitive measures.[44] The European Court of Justice (ECJ) qualified sanctions as "temporary precautionary measures"[45] and in the seminal Kadi II highlighted their preventive nature.[46] By their preventive purpose, they are different from criminal sanctions and aim at supporting international peace and security.[47] Since the purpose of sanctions is prevention, a listed legal or natural person shall not be an official suspect of a crime or subject of criminal procedure. The assets of the persons concerned are not confiscated as the proceeds of a crime, but frozen as a precautionary measure.[48] The blacklist is conceptualized as targeting an enemy rather than a rulebreaker.[49] A similar approach to sanctions as preventive measures is pursued by the UN. The UN Security Council does not need to establish a breach of an international obligation for the enactment of sanctions[50] but only a "threat to the peace, a breach of the peace or an act of aggression" within the meaning of Article 39 of the UN Charter.[51]

The Court has also previously rejected arguments stemming from the criminal law in sanctions litigations, i.e. the compliance of sanctions with the presumption of innocence and the principle that penalties must fit the offence. In its judgement in El Morabit the Court highlighted that the presumption of innocence does not prevent the imposition of a precautionary measure with a preventive aim such as asset freezes.[52] Furthermore, in this case

---

[44] Council of the European Union, Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy 5664/18 (2018), para 45.
[45] Joined Cases C-539 & 550/10 P, Al Aqsa v. Council and Netherlands v. Al Aqsaj ECLI:EU:C:2012:711 (2012), para 120.
[46] Kadi II, para 130.
[47] Case T-439/11 Sport-Pari v Council [2014] ECLI:EU:T:2014:1043, para 89; Case T-256/11 Ezz and Others v Council [2014] ECLI:EU:T:2014:93, paras 77-80; Case T-619/15 Bureau d'achat de diamant Centrafrique v Council [2017] ECLI:EU:T:2017:532, para 71 ; Case T-128/12 et T-182/12 HTTS v Council [2013] ECLI:EU:T:2013:312, para 42.
[48] Ibid.
[49] Eva Nanopoulos, The Juridification of Individual Sanctions and the Politics of EU Law (Bloomsbury Publishing, 2020).
[50] Tom Ruys, 'Sanctions, Retorsions and Countermeasures: Concepts and International Legal Framework' in Larissa van den Herik (ed), Research Handbook on UN Sanctions and International Law (Edward Elgar Publishing 2016) 19.
[51] Hans Kelsen, 'Collective Security and Collective Self-Defense Under the Charter of the United Nations' (1948) 42(4) The American Journal of International Law 783, 789.
[52] El Morabit v. Council CFI joined cases T-37/07 and T-323/07, ECLI:EU:T:2009:296 (2009) para 40.

the Court stated that asset freezes are preventive measures and do not constitute sanctions.[53] This was the first time that the court explicitly highlighted the non-criminal nature of asses freezes.[54]

In the Ipatau case, the Court rejected the applicant's argument that his inclusion on the sanctions list is illegal since his individual responsibility was not proven[55] and, according to the principle that penalties must fit the offence, he could be penalized only for acts imputed to him individually.[56] Here again the Court insisted on the preventive nature of sanctions as foreign policy measures that do not entail a decision of guilt.[57] The Court makes a clear distinction between restrictive measures that are purely preventive and adopted within an administrative procedure and criminal sanctions that imply a statement of guilt.[58]

3.3. Severity of the penalty : EU measures are punitive

Another element to look at while examining whether EU restrictive measures could qualify as criminal is the penalty that they imply. In the past, the long duration of counter-terrorism sanctions has raised questions as to their preventive administrative nature.[59] Sanctions have been labelled "draconian measures, unlimited as to time and quantum", as having "devastating" consequences.[60] Van Aaken compared longer-term asset freezing, without due process, to an expropriation.[61] If sanctions are unlimited measures as to their duration, they risk having serious consequences for listed individuals and, thus, resemble punitive measures. For instance, they entail a considerable restriction of the exercise of the listed individual's right to property.[62]

While sanctions are conceived to be limited in time and be lifted once their objectives are fulfilled, in practice they seem to be unlimited as to their duration.[63] This is often due to the fact that it is unclear what constitutes a benchmark for sanctions to be lifted. The 2018 Council sanctions guidelines set out that "restrictive measures are imposed by the EU to bring about a change in policy or activity by the target country, part of country, government, entities or individuals".[64] Some scholars, however, consider that the objective of changing policy or activity is a relic from the times that sanctions were necessarily connected to the political

---

[53] El Morabit, para 40.
[54] Van den Broek, Hazelhorst, and de Zanger, 'Asset Freezing', 24.
[55] Ipatau v Council, cit. para 108-110.
[56] Ibid. para 112; Case T-38/02 Groupe Danone v Commission ECLI:EU:T:2005:367 paras 277 -278.
[57] El Morabit para. 43
[58] El Morabit, para. 44; See van den Broek, Hazelhorst, and de Zanger, 'Asset Freezing'.
[59] Cameron, "The European Convention on Human Rights, Due Process and United Nations Security Council Counter-Terrorism Sanctions" (Report to the Council of Europe, 2006).
[60] A.G. Maduro, Opinion in Case C-402/05 P Yassin Abdullah Kadi v Council of the European Union and Commission of the European Communities ECLI:EU:C:2008:11 (2008) para 47.
[61] A. van Aaken, 'International investment law and decentralized targeted sanctions: an uneasy relationship', Columbia FDI Perspectives No. 164, (2016), available at http://ccsi.columbia.edu/files/2013/10/No-164-van-Aaken-FINAL.pdf
[62] Joined Cases C-539 & 550/10 P, Al Aqsa v. Council and Netherlands v. Al Aqsaj ECLI:EU:C:2012:711 (2012) para 120.
[63] Yuliya Miadzvetskaya, Celia Challet. Are EU restrictive measures really targeted, temporary and preventive? The case of Belarus.
[64] Council of the EU, Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy 5664/18 (2018), para 4.

regime of a third country.[65] While change of a regime or a policy can be induced from objective factors, it is unclear what constitutes a change of an individual behavior.[66]

Such a change of behavior is even more difficult to asses with respect to cyber-attacks. First of all, it is unclear what this change of behavior implies specifically. Secondly, the delimitation between State and non-State actors in cyberspace is challenging. Some hackers do not act in their name but as proxies under the instructions of governments. What would be the benchmark to establish that hackers changed their behavior and will restrain from cyber operations in the future? Furthermore, In this specific case, what change of behavior is expected, and from whom more specifically? Changing policy or an activity with respect to individual hackers is not a realistic goal. Given that those questions will most probably remain unanswered in the near future, it is possible to conclude that restrictive measures under the cyber sanctions regime are of an unlimited duration. This brings them closer to punitive measures.

In addition to the punitive nature of cyber sanctions stemming from their unlimited duration, two other distinct features can be identified, notably the triggering situation and the timeline of a sanctioned act. They bring sanctions in response to cyberattacks closer to punitive measures.

The main trigger for the introduction of cyber sanctions is different from other country-specific sanctions frameworks. The first difference lies in the territorial dimension of sanctions in response to cyberattacks. While most EU sanctions are enacted in response to a triggering situation that takes place outside the EU territory and presents an indirect threat to EU security, both thematic sanctions frameworks on cyber-sanctions and the use of chemical weapons address respectively inter alia situations that took place on the EU territory and implied economic losses and bodily harm to EU citizens and residents. The Novichok agent used for the Skripal poisoning presented a direct threat to the national security of one Member State and its residents. Cyber-attacks such as NotPetya also bear important losses for the EU economy and imply security risks for Member States.

The second distinctive feature of sanctions in response to cyberattacks resides in the timeline of the sanctioned act. It would be fair to say that cyber-sanctions are similar in this sense to other thematic sanctions framework since they seek to address a specific act that took place in the past. In that sense sanctions in response to cyberattacks target a specific conduct or a misbehaviour whereas some other sanctions regimes address a rather hypothetical threat that has not materialised yet. For instance, sanctions against Iran nuclear program accomplish their preventive function by containing Iran and signalling that a threat has been detected. Sanctions in response to cyberattacks serve as an instrument of deterrence, prevention and punishment with respect to malicious cyber actors that have taken place or have been mitigated.

4. EU sanctions in response to cyber-attacks: preventive in nature but punitive in effect[67]

It follows from the previous section that sanctions are preventive in nature but punitive in some elements of their design and effects. In this respect cyber sanctions accomplish an important function as an instrument of crime prevention. More specifically they compliment

[65] Christina Eckes, 'EU Human Rights Sanctions Regime: Ambitions, Reality and Risks' (2020) 64 Amsterdam Law School Research Paper, 8.
[66] Ibid.
[67] Inspired by Francesca Galli, The freezing of terrorists' assets: preventive purposes with a punitive effect.

criminal law rules when their efficiency is impacted by the impossibility to reach foreign hackers abroad. Furthermore, sanctions in response to cyber-attacks could be viewed as 'quasi counter-measures' since they aim at punishing and signalling the inappropriate behaviour in cyberspace.

4.1. Sanctions in response to cyber-attacks as complementary instruments of crime prevention

Under the EU legal framework two avenues are available in order to hold accountable those who are involved in malicious cyber activities. One route is to adopt sanctions under the CFSP. Another one is to proceed through criminal measures since computer crime is listed as one of crimes under Article 83(1) TFEU. Since cybercrime is punished under criminal law, it is interesting to explore whether sanctions in this context fulfil a role of mere substitute or complementary measures for the punishment and deterrence of cyber criminals who are out of reach for European authorities.

In the past years we could witness a considerable harmonisation of national laws with respect to the definition of computer crime and penalties in response to internet crimes. The EU has in place the 2005 Council Framework Decision on attacks against information systems[68] and the 2013 Cybercrime Directive.[69] The Cybercrime Directive contributes to the judicial cooperation in criminal matters and provides for minimum rules on the definition of criminal offences and sanctions in response to attacks against information systems. Those include access to systems, systems interferences, data interference and can be criminalised with penalties from two to five years.[70] It also sets out a procedure in its Article 12 on the basis of which a Member State must inform the Commission how it establishes its jurisdiction over offences outside its territory.

Despite all the harmonisation efforts in the criminal realm, it is often impossible to hold foreign hackers accountable before the EU courts. Similar situation can be observed in the US. The Justice Department regards the indictments of foreign hackers as a way to "name-and-shame" them and deter their malicious activities.[71] At the same time, the deterrent potential of indictments is questionable since the cases of foreign hackers being brought before the US Courts for trials are limited. There are some exceptions like the Ukrainian hacker Yaroslav Vasinskyi who was detained after he travelled to Poland. Once put on the wanted list, foreign hackers are locked in in their home countries to some extent.

In this respect, EU cyber sanctions act as complementary crime prevention measures to target cyber-attacks that represent an external threat[72] and imply the following violations: unauthorized actions that involve access to information systems, information system interference, data interference or interception.[73] The listed unauthorized activities

[68] Council Framework Decision 2005/222/JHA on attacks against information systems (2005) OJ L 69/67.
[69] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218 (Cybercrime Directive).
[70] Art. 9 Cybercrime Directive.
[71] Eric Tuckler, 'FBI, US agencies look beyond indictments in cybercrime fight' (AP 2022) https://apnews.com/article/technology-indictments-crime-europe-hacking-8e97ebd22a64a28bfc4ea83c123ee1dc.
[72] Council Decision (CFSP) 2019/797, art. 1(2)(4).
[73] Council Decision (CFSP) 2019/797, art. 1(3).

qualify as a computer crime under EU law and can be divided into three groups of malicious activities. The first group includes virus and ransomware attacks that gain access to information systems and/or data and destroys, encrypts or locks data stored on the device.[74] The second category encompasses unauthorized access to information systems or data, better known as hacking.[75] The third group of sanctioned activities is the distributed denial of service (DDOS) that consist in overwhelming computer possibilities with a large number of requests.[76]

For the time being, eight natural persons and four entities or bodies are targeted by EU restrictive measures as being responsible for the attempted cyber-attacks against the OPCW and the cyber-attacks publicly known as 'WannaCry' and 'NotPetya', as well as 'Operation Cloud Hopper', and the cyber-attack on the German Federal Parliament (Deutscher Bundestag) in April and May 2015.[77]

4.2. Sanctions in response to cyberattacks as quasi counter-measures?

The viewpoint on EU sanctions as exclusively preventive measures is difficult to square with the fact that they are increasingly formulated as reactions to prior breaches of rules of responsible State behaviour in cyberspace. From the point of view of international law sanctions in response to cyber-attacks could potentially qualify as counter-measures.[78] However, since the application of the current legal framework to cyber-attacks is still underspecified, it would be difficult to establish a specific rule of international law that could be violated as a result of a cyber operation.

Furthermore, the EU does not have procedures in place for the attribution of responsibility for cyber-attacks to third countries. Discussions on this topic are out of question at the moment since there is no political will to establish common attribution procedures. Sanctions, mentioned in the Cyber Diplomacy Toolbox, are targeted measures aimed at individuals, groups or companies and they do not lead to the attribution of responsibility to a State. While the guidelines of the Council of October 2017 initially referred to the possibility of the adoption of sanctions against a State when it carries out the malicious cyber activity or when it is deemed responsible for the actions of a non-state actor,[79] the May 2019 Council Decision emphasises the targeted nature of restrictive measures, excluding any attribution of

---

[74] Troy Anderson, 'Fitting a Virtual Peg into a Round Hole: Why Existing International Law Fails to Govern Cyber Reprisals' (2017) 34(1) Ariz. J. Int'l & Comp. L., 135-157, 136.
[75] Ibid.
[76] Ibid.
[77] Council Decision (CFSP) 2020/1127 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (2020) OJ L 246; Council Decision (CFSP) 2020/1537 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (2020) OJ L 351I; Council Decision (CFSP) 2020/1748 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (2020) OJ L 393.
[78] More on sanctions as counter-measures see Tom Ruys, 'Sanctions, Retorsions and Countermeasures: Concepts and International Legal Framework'.
[79] Council Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities (2017) cit. 20.

responsibility for cyber-attacks to a third State.[80] Nevertheless, Member States are free to make their own determinations with respect to the attribution of cyberattacks. And contrary to some Member States, which publicly attributed cyber-attacks to specific states, the EU has not taken any act of attribution or follow up with regard to potential perpetrators.[81]

The targeted nature of cyber sanctions allows the EU to avoid the sensitive question of attribution of responsibility for cyber-attacks to a third country within the currently still underspecified international legal framework governing this area. As individual designations circumvent the establishment of state responsibility, the EU has *de facto* never attributed a cyber-attack to a third country, but has limited its actions to the expression of concerns and condemnations.

However, the delimitation between targeted measures and attribution of responsibility to a state remains rather superficial since a vast majority of cyber-attacks with high impact, such as the abovementioned 'WannaCry' and 'NotPetya', were widely understood to have been orchestrated at the request and with the support of governments of, allegedly, North Korea and Russia respectively. I would argue that individual listings under the cyber-sanctions framework could be compared to the indirect attribution of responsibility to States since all actors sanctioned have a clear connection with a specific State. The EU has indeed attributed responsibility for cyber-attacks to individuals who worked for State bodies. As an example, the EU sanctioned four Russians among them one is the current Head of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), while others work at different levels for the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU). Other sanctioned individuals and entities are connected to APT10 or APT38 known as a Chinese and North Korean state-sponsored threat group that specialises in cyber operations.

5. Concluding remarks

The present paper demonstrated that restrictive measures broadly and sanctions in response to cyber-attacks specifically, despite their growing personification and allegedly punitive nature, are not criminal measures from the point of view of procedural and evidence related standards. First of all, despite the recognition of a computer crime as a crime that could be punished with imprisonment and fines, sanctions under the Common Foreign and Security Policy constitute a different type of instruments. They are foreign policy measures enacted on the basis of Article 29 TEU and 215 TFEU by the EU for ensuring the State responsible behaviour in cyberspace and serve as a cyber deterrence instrument.

Secondly, it is undeniable that sanctions in response to cyberattacks tend to be unlimited as their duration. In that sense they risk having serious consequences for listed individuals and, thus, resemble punitive measures by considerably restricting the exercise of the listed individual's right to property.[82] Nevertheless, this sole penalty related criteria is not sufficient

[80] Council Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (2019).
[81] Paul Ivan, 'Responding to cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox' (European Policy Center 2019) <http://www.epc.eu/pub_details.php?cat_id=17&pub_id=9081> accessed 6 June 2019.
[82] Joined Cases C-539 & 550/10 P, Al Aqsa v. Council and Netherlands v. Al Aqsaj ECLI:EU:C:2012:711 (2012) para 120.

for calling sanctions as punitive measures. It would be fair to acknowledge their preventive nature with punitive effects though.[83]

The debate on whether EU sanctions amount to punitive or criminal measures is important given the contemplated changes in the EU sanctions practice, notably the potential confiscation of frozen assets and qualification of sanctions evasions as a crime under Article 81(3) TFEU. The EU legislators seem to look for any possible legal anchor justifying the seizure of Russian assets. Nevertheless, there is a number of arguments in favour of keeping sanctions rather preventive than punitive. First of all, their preventive nature allows to react to emergency situation like for instance cyber-attacks, the forced landing of the Ryanair plane or the unexpected Russian war against Ukraine. The recognition of the punitive nature of sanctions would involve the cumbersome complexity of a lengthy criminal justice process.

[83] Francesca Galli, The freezing of terrorists' assets: preventive purposes with a punitive effect

Alessandro Cortina (2023): Beyond a techno-centric vision of cybersecurity. In: EU Cybersecurity: Collective Resilience through Regulation, June 22nd 2023, Brussels - Belgium

Beyond a techno-centric vision of cybersecurity

Alessandro Cortina
Information Society Law Center (ISLC) – University of Milan (Italy)
alessandro.cortina@guest.unimi.it

Abstract

Recent European Union regulations dealing with cybersecurity issues focused not only on technical but also organizational aspects, by explicitly recognizing the need for stakeholders affected by these regulations to address not only the technical aspects of cybersecurity, and by encouraging the development of a holistic approach to tackle the daily challenges of cybersecurity.

The aim of this research is to highlight the importance of organizational aspects within a cybersecurity strategy by going against the techno-centric view of the information security problem still predominantly prevalent in the industry.

In fact, analyzing some surveys that have been carried out both at the Italian national level (Macinante & Longo, 2021) (The Innovation Group, 2022) and at the international level (SPLUNK, 2022) (ISACA, 2022), there would appear to still be a prevailing view that professionals in the field identify the problem of cybersecurity as an issue mainly concerning technical matters and, in addition, matters concerning research and training of qualified personnel. For example, in "The State of Security 2022" survey conducted by SPLUNK, to the question

"Why Security Keeps Getting Harder?" among the most frequent answers given by respondents were the following:

(1) "Our security stack and the number of tools/vendors in use has become overwhelmingly complex".

(2) "We are increasingly struggling to find/hire enough skilled security resources to handle the workload".

(3) "We are too busy fighting daily attacks to refine our tools and processes to support the expanding attack surface and threat landscape". However, it is believed that continuing to "look" at the cybersecurity from only one perspective, the technical one, can only lead to fallacious and incomplete defense strategies.

Contextually with highlighting this concept, this paper also emphasizes how the socio-technical organizational approach can be a valuable ally in overcoming such a techno-centric view of the cybersecurity "problem." However, the use of socio technical systems theory principles in relation to cybersecurity issues would not be a new element. On the contrary, it is precisely because of their already proven use that their usefulness is highlighted. In fact, the socio-technical approach has been validly used in several areas pertaining to the world of cybersecurity. For example, through this approach, initiatives have been developed: both in the area of designing strategic defense plans at the national level and in the area of fighting cybercriminals (Kowalski, 1991) (Ghernaouti-Hélie, 2009) (Schjølberg & Ghernaouti-Hélie, 2011) (Odumesi, 2014) (Zhang, Tang, & Jayakar, 2018). In addition, it is well established in the literature the use of the socio-technical approach for the analysis of organizational incidents (Vaughan, 1996) (Mason, 2004) (Catino, 2006). And it is precisely by following this approach that it is possible to discern the cruciality of the organizational component in the successful implementation of a security strategy. Think of the cyber incidents such as the Equifax case and the WannaCry case in relation to the UK's National Health Service (NHS). In the first case, a whole series of delays in the execution of the work and lack of attention by top management to the issue of security led to the

exfiltration of personal data related to about 148 million people (Kabanov & Madnick, 2021) (Staff Report: Permanent Subcommittee on Investigations, 2019). However, in the second case the lack of adequate crisis management plans, inadequate security infrastructure of the various local entities linked to the NHS, and a lack of sensitivity of the British government on the issue led to a massive unavailability in being able to deliver the appropriate care to patients (House of Commons Committee of Public Accounts, 2018). These two cases are emblematic of how an accidental event could have been avoided by simply adopting proper organizational measures. Although the technical issues were the spark that ignited the explosion, nevertheless organizational deficiencies allowed the conditions to be created for said accidents to occur.

Such incidents highlight how the problem of cybersecurity, but also of security in general, is an issue that needs to be addressed with a holistic approach, as an ideology whereby cybersecurity is solved through the adoption of technological measures (however sophisticated they may be) and merely by carrying out awareness campaigns for an organization's users can no longer be contemplated (Whitten & Tygar, 1999) (Ford, 1994) (Gordon, 1995) (Adams & Sasse, 1999). On the topic of user education and the concept of awareness, in addition, there is another aspect to be explored. Indeed, it is believed that the conception that human beings are the weak component of the security chain should be demystified and that there is nothing that can be done to overcome this view. In fact, progress should be attempted from the conception of the human operator in relation to safety issues coming from the field of Reliability engineering and also taken up later by the engineering approach in the field of accident causation theory (ENISA, 2018) (Catino, 2006) (Gherardi, Nicolini, & Odella, Dal rischio alla sicurezza: il contributo sociologico alla costruzione di organizzazioni affidabili, 1997) (Gherardi, Nicolini, & Odella, La cultura della sicurezza sui luoghi di lavoro, 1997). Continuing to label the human being as the uncontrollable element within a process because of its unpredictability and the impossibility of codifying its behavior, and thus achieving deterministic behavior (the same input will always result in the same output), only prevents progress toward new security strategies in which the human component plays a central role and in which the

individual human operator is made accountable for its own actions and becomes, therefore, an integral part of the security infrastructure. Hence, one agrees with what V. Zimmermann and K. Renaud (2019) stated on this point. The authors precisely highlighted the difference between the (basically) techno-centric approach, currently still widely used and referred to by them as "Cybersecurity Currently", and the approach they propose that embraces the socio-technical philosophy and referred to as "Cybersecurity Differently". In the first approach, the authors emphasize how the human operator is seen as a problem in the security chain, thus debasing its nature and depriving it of the opportunity to enhance the quality of the security system. In contrast to the paradigm of *"human as a problem"*, in relation to the *"Cybersecurity, Differently"* the authors talk instead of *"human as a solution"*, attributing to the human component the ability to improve the security system and to be an integral and active part of it. Even ENISA identified the human factor as an element to be valorized since, with particular reference to the issue of security culture within an organization, it was observed that the growth of sensitivity to security issues on the part of personnel then has beneficial repercussions both at group and organizational level (ENISA, 2018).

Considering the foregoing considerations, further reflection is also encouraged. In particular, in the same way that an organization's business is affected by solicitations from the external environment (new competitors, issues in the supply of raw materials, etc.), an organization's security systems and related processes are also affected by such external solicitations. In fact, R. Anderson (1994) already highlighted this concept. In particular, the author analyzed the impact of financial regulations on bank liability with the security measures taken by credit institutes. The author correlated the US system with the British system (among others mentioned in the contribution): in the former, the responsibility for the costs of fraud falls on the banks, which in the event of a dispute over a customer's transaction must compensate the customer unless they can prove fraudulent conduct on their part in order to deceive the bank; in the second, on the other hand, an attitude favorable to the banks developed and consolidated, such that when faced with a customer claiming compensation for a transaction, it was the latter

who had to "prove" that he had nothing to do with the matter and that he was really the victim of fraud. The aforementioned study highlights how a different social and legal environment resulted in different approaches to security, which led to the British banking system paradoxically facing more fraud than the US system, as British lenders 'with an advantageous position' over their customers had not invested properly in the continuous improvement of their security system. This evidence leads, therefore, to the following consideration:

(1) an organization is affected by solicitations from its surroundings; (2) as security is an internal process within the organization, it will be affected by the effects of such solicitations, too;

(3) as a result, the changes that the organization must adopt for security adaptation to external solicitations will have to be hybrid in nature. Such a view leads to the assertion that responding to external stresses by adopting only technical changes, so changes of only one kind, would mean failing to respond properly to all solicitations received from the external environment. In conclusion, to effectively address current and future cybersecurity issues, which will become increasingly compound as the complexity of our society grows, it will be crucial to move beyond the techno-centric model of conception of cybersecurity and embrace a holistic approach in which social and organizational issues are also identified as issues to be addressed as most important. To do this, the impulse of European policy making represents a significant lever that may (and should) be used to vehiculate the work, studies and attention of practitioners in the field.

References

Adams, A., & Sasse, M. A. (1999): 'Users are not the enemy. Why users compromise computer security mechanisms and how to take remedial measures', *Communications of the ACM*, vol. 42, no. 12, pp. 40-46.

Anderson, R. J. (1994): 'Why Cryptosystems Fail', *Communications of the ACM,* vol. 37, no. 11, pp. 32-40.

Catino, M. (2006): *Da Chernobyl a Linate: incidenti tecnologici o errori organizzativi?* B. Mondadori.

ENISA. (2018): *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity.* ENISA. Ford, W. (1994): *Computer Communications Security: Principles, Standard Protocols and Techniques,* Prentice Hall, New Jersey.

Gherardi, S., Nicolini, D., & Odella, F. (1997): 'Dal rischio alla sicurezza: il contributo sociologico alla costruzione di organizzazioni affidabili', *Quaderni di sociologia,* no. 13, pp. 79-108.

Gherardi, S., Nicolini, D., & Odella, F. (1997): 'La cultura della sicurezza sui luoghi di lavoro', *Sviluppo & Organizzazione,* no. 162, pp. 15-30.

Ghernaouti-Hélie, S. (2009): 'An Inclusive Information Society Needs a Global Approach of Information Security', *2009 International Conference on Availability, Reliability and Security*, pp. 658-662.

Gordon, S. (1995): 'Social Engineering: Techniques and Prevention', *Proceedings of the 12th World Conference on Computer Security, Audit & Control*, pp. 445-451.

House of Commons Committee of Public Accounts (2018): *Cyber-attack on the NHS: Thirty Second Report of Session 2017–19.* House of Commons.

ISACA (2022), *State of Cybersecurity 2022,* ISACA.

Kabanov, I., & Madnick, S. (2021): 'Applying the Lessons from the Equifax Cybersecurity Incident to Build a Better Defense', *MIS Quarterly Executive,* vol. 20, no.2, pp. 109-125.

Kowalski, S. (1991): 'The SBC model: modeling the system for consensus', *Proceedings of the 7th IFIP TC11 Conference on Information Security,* Brighton (UK), pp. 1-7. Macinante, R., &

Longo, M. (2021): *Barometro Cybersecurity 2021.* NetConsulting Cube.

Mason, R. O. (2004): 'Lessons in Organizational Ethics from the Columbia Disaster: Can a Culture be Lethal?', *Organizational Dynamics,* vol. 33, no. 2, pp. 128-142.

Odumesi, J. O. (2014): 'A socio-technological analysis of cybercrime and cyber security in Nigeria', *International Journal of Sociology and Anthropology,* vol. 6, no. 3, pp. 116-125.

Schjølberg, S., & Ghernaouti-Hélie, S. (2011): *A Global Treaty on Cybersecurity and Cybercrime (2nd Edition).* AitOslo, Oslo.

SPLUNK (2022): *The State of Security 2022,* SPLUNK.

Staff Report: Permanent Subcommittee on Investigations (2019): *How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach,* United States Senate.

The Innovation Group (2022): *Cyber Risk Management Survey 2022,* The Innovation Group.

Vaughan, D. (1996): *The Challenger launch decision: Risky technology, culture, and deviance at NASA,* University of Chicago press, Chicago.

Whitten, A., & Tygar, J. D. (1999): 'Why Johnny Can't Encrypt: A Usability Evaluation of PGP', 5.0. *Proceedings of the 8th USENIX Security Symposium*, pp. 169-184.

Zhang, H., Tang, Z., & Jayakar, K. (2018): 'A socio-technical analysis of China's cybersecurity policy: Towards delivering trusted e-government services', *Telecommunications Policy,* vol. 42, no. 5, pp. 409-420.

Zimmermann, V., & Renaud, K. (2019): 'Moving from a "human-as-problem" to a "human-as solution" cybersecurity mindset', *International Journal of Human-Computer Studies,* vol. 131, pp. 169-187.

N.M Brouwer (2023): The EU Cyber Security Strategy: Breaking the Vicious Circle of Cyber Insurance? In: EU Cybersecurity: Collective Resilience through Regulation, June 22nd 2023, Brussels - Belgium

The EU Cyber Security Strategy: Breaking the Vicious Circle of Cyber Insurance?

Dr N.M. Brouwer
Radboud University Nijmegen, The Netherlands
nynke.brouwer2@ru.nl

Part 1: Consolidating cyber insurance: A vicious circle?

The increasing use of digital technologies and the dependence of modern society on digital services and products has given rise to a wide range of new security risks, which can result in major losses and damages for businesses and organisations, as well as for society in general. Security incidents, which I will call 'cyber incidents', can compromise the confidentiality, integrity, and availability of information and information systems, causing data breaches, business interruption, monetary losses, reputational damage, and enforcement and civil liability risks. Given the potentially severe impacts of cyber incidents, simply managing such risks by mitigation, avoidance or retention is not enough. Therefore, transferring or sharing risks by purchasing insurance coverage is a necessary complement to companies' risk management strategies.

In general, insurance mechanisms can contribute to adequate cyber risk management systems by "promoting awareness, encouraging measurement, and by providing incentives for risk reduction." (OECD, 2017). Insurers are in a unique position to encourage positive behavioural change, for instance by requiring specific security standards to enter into insurance contracts, or by rewarding good behaviour while sanctioning bad behaviour (i.e. a bonus/malus system). Insurance has the potential to contribute to an overall higher level of security (Brouwer, 2021; Woods and Moore, 2020).

Cyber insurance has been on the rise for several decades now, varying from add-ons to traditional insurance policies like property policies or professional error & omissions policies, to stand-alone cyber insurance (Brouwer, 2021; Wolff, 2022; Tshohou et al., 2023). Cyber insurance policies provide coverage for a broad range of risks, as well as what Wolff describes as an "astonishing number of different types of damages" (Wolff, 2022). Indeed, one of the characteristics of cyber insurance is its hybridity, as it covers first-party losses as well as third-party damages, which vary from data losses and breach notification costs, reputational damage, ransom payments, regulatory fines, and business interruption costs, to liability claims and lawsuits (Brouwer, 2021; Wolff, 2022). Likewise, the covered risks can stem from cybercrime like hacking, malware, or digital theft and extortion, but also from human errors or network outages.

Several elements are causing challenges for cyber risk insurance. Firstly, cyber risks are highly unpredictable, as they are subject to rapid technological changes while being interdependent, accumulative, and therefore potentially catastrophic. Secondly, cyber risks are unprecedented. Unlike traditional policies, there is no broad consensus on how key concepts in policy wordings should be defined. In addition, there is only a relatively limited claims history for insurers to analyse in order to calculate adequate premiums. This lack of data is a key challenge for the further development and maturing of the cyber insurance market (OECD, 2020). This problem causes the so-called vicious circle of cyber insurance. This circle starts with the observation that insurers have not yet collected a critical amount of loss data and that, for several reasons, many cyber incidents are not reported at all. Furthermore, the covered risk is constantly evolving, making it hard to reach consensus about adequate security measures. The lack of data makes insurers cautious in underwriting and pricing the risks, leading to vague policy wordings and restricted coverage. This is problematic for potential cyber insurance clients,

leading to a low take-up rate. Since relatively few policies are sold, little data is generated, which brings us back to the beginning of the problem.

The lack of data with regard to adequate cybersecurity measures and information sharing has hindered the cyber insurance market in reaching further maturity. There have been several calls for improvement, e.g. by ENISA, who recommended using existing regulatory frameworks such as the General Data Protection Regulation and the Network and Information Security Directive to develop a common framework, as well as using these regulations' mandatory incident reporting schemes to produce meaningful data (ENISA, 2017). In addition, insurers as well as policymakers should promote and improve communication and information sharing, e.g. via Information Sharing and Analysis Centres (ENISA, 2017). The Organisation for Economic Co-operation and Development has also stated that the cyber insurance industry might benefit from data sharing initiatives, but acknowledges that anti-trust and data protection regulations might inhibit this, as well as the unwillingness of large underwriters and reinsurers to participate in incident or claims data sharing initiatives (OECD, 2020; Tshohou, 2023). The European Insurance and Occupational Pensions Authority has advocated for a European cyber incident-reporting database as well (EIOPA, 2019). Specific research from The Netherlands shows that public disclosure of data breach notifications could increase social welfare (Nieuwesteeg, Van Eeten and Faure, 2018). Other scholars have likewise stated that "requiring organisations to have cybersecurity measures and report cyber incidents is not only advisable, it will be key to ensuring the survival of cyber insurance" (Nieves, 2020; Puławska, Strzelczyk and Orzechowski, 2022), and that a majority of representatives in the cyber insurance market "agree that cyber-attack data should be collected in a database accessible to all insurers." (Puławska, Strzelczyk and Orzechowski, 2022).

Part 2: The EU Cyber Security Strategy's provisions in cyber security measures and data sharing

While the cyber insurance market is struggling with the challenges described above, the European Commission's development of cyber-related legislation is flourishing. The EC is presenting a comprehensive strategic and accompanying legal framework for the digital domain, covering such aspects as data

management, digital services, privacy, artificial intelligence, cyber security and product safety. Indeed, the EC claims that the Cyber Security Strategy "forms a key component of Shaping Europe's Digital Future" of the European Union (European Commission, 2020). It aims to implement an extensive set of instruments that cover many different aspects of cyber security, emphasizing resilient infrastructure and critical services, and employing the development of secure technologies across the whole supply chain (i.e. cybersecurity by design for industrial processes, operations and devices) as an accelerator for increasing resilience (European Commission, 2020). Additionally, the Cyber Security Strategy highlights the importance of information sharing, proposing to build a network of Security Operations Centres across the EU by encouraging Member States to invest in Information Sharing and Analysis Centres, which eventually serve as a 'Cybersecurity Shield' for the EU (European Commission, 2020). Important legislative corollaries of the European Strategy are the Cybersecurity Act,[1] the revision of the Network and Information Security Directive (NIS II),[2] the Digital Operational Resilience Act (DORA),[3] the proposals for a Cyber Resilience Act[4] and an Artificial Intelligence Act[5] and its AI Liability Directive,[6] and lastly the revised Product Liability Directive.[7]

Part 3: The dynamics between regulation and insurance: research question and methodology

While the EU Cyber Security Strategy does not explicitly aim to facilitate the development of the cyber insurance market, it does address various aspects with which this market is struggling, particularly in relation to increasing cyber resilience by harmonizing cybersecurity measures and sharing information. Likewise, the EU strategy and legislative initiatives aim to influence the (cyber) risk exposure of organizations throughout the EU, to which the insurance market by definition also seeks to respond. Undeniably, then, there are interactions between the proposed legislation and the cyber insurance market.

---

1 Regulation (EU) 2019/881.
2 Directive (EU) 2022/2555.
3 Regulation (EU) 2022/2554.
4 Proposal for a Regulation, 15 September 2022, COM(2022) 454 final.
5 Proposal for a Regulation, 21 April 2021, COM(2021) 206 final.
6 Proposal for a Directive, 28 September 2022, COM(2022) 496 final.
7 Proposal for a Directive, 28 September 2022, COM(2022) 495 final.

In this paper, I will examine to what extent the EU Cyber Security Strategy for the Digital Decade can contribute to solving key problems in the development of the cyber insurance market. I will therefore assess which legislative initiatives within the Cyber Security Strategy directly or indirectly influence the cyber insurance market, by identifying and analysing provisions about cybersecurity measures and information sharing systems. In what ways do these legislative provisions contribute to the harmonization of cyber security measures and incident data sharing, and what are their blind spots? And to what extent are cyber insurers possibly already ahead of these legislative provisions?

The structure of the contribution will be:

(1) Introduction;
(2) Key problems for the cyber insurance market (as described in this abstract);
(3) The EU Cyber Security Strategy and its legislative framework;
(4) Specific legislative provisions on cybersecurity and information sharing;
(5) Implications of these provisions for the cyber insurance market;
(6) Conclusion.

References

Brouwer, N.M. (2021): *De cyberverzekering vanuit civielrechtelijk perspectief*, Wolters Kluwer, Deventer.

EIOPA (2019): *Cyber Risks for Insurers – Challenges and Opportunities*, Publications Office of the European Union, Luxembourg.

ENISA (2017): 'Commonality of risk assessment language in cyber insurance – Recommendations', 15 November 2017, https://www.enisa.europa.eu/publications/commonality-of-risk-assessment-language-in-cyber-insurance.

European Commission (2020): *Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade*, 16 December 2020, JOIN(2020) 18 final.

Nieuwesteeg, B., Van Eeten, M. and Faure, M. (2018): *Scientific research data breach notification obligation*, 29 November 2018.

Nieves, A.M. (2020): 'Cyber Insurance Today: Saving It before It Needs Saving', *The Catholic University Journal of Law & Technology*, vol. 29, no. 1, Fall 2020, pp. 111-144.

OECD (2017): *Supporting an effective cyber insurance market*, OECD Report for the G7 Presidency, https://www.oecd.org/daf/fin/insurance/Supporting-an-effective-cyber-insurance-market.pdf.

OECD (2020): *Enhancing the Availability of Data for Cyber Insurance Underwriting*, www.oecd.org/finance/insurance/Enhancing-the-Availability-of-Data-for-CyberInsurance-Underwriting.pdf.

Puławska, K., Strzelczyk, W. and Orzechowski, A. (2022): 'Cyber insurance and information sharing as prevention from cyber-attacks – pilot study', 28 October 2022, https://ssrn.com/abstract=4260821.

Tshohou, A. et al. (2023): 'Cyber insurance: state of the art, trends and future directions', *International Journal of Information Security*, 16 January 2023, https://doi.org/10.1007/s10207-023-00660-8.

Wolff, J. (2022): *Cyberinsurance policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks*, The MIT Press, London.

Woods, D.W. and Moore, T. (2020): 'Does insurance have a future in governing cybersecurity?', *IEEE Security & Privacy*, vol. 18, no 1, pp. 21-27.