SANCTIONS MECHANISMS ADRESSING CYBERSPACE: AN ANALYSIS OF THE APPROACHES OF THE EUROPEAN UNION AND THE UNITED NATIONS

PETRA LUKAČOVIČOVÁ

Abstract: The presented article analyses the legal basis, structure, and application of sanctions mechanisms within the EU and UN in the context of cyber operations. The article focuses on sanctions mechanisms that are activated based on the process of attribution of state responsibility for cyber operations. It discusses the specifics and unique aspects of both organisations, while trying to point out their most fundamental differences. The aim of this article is to qualitatively compare the effectiveness of EU and UN sanctions mechanisms, thereby demonstrating differences in their output depending on their degree of legally binding nature.

Keywords: cyberspace; cyber sanctions; EU; UN

DOI: 10.14712/23366478.2026.96

INTRODUCTION

The topic of cyber warfare resonated long ago before it even became an issue. Due to many international crisis and problems, it was pushed to the sidelines. Cyber operations are still more common and the trend seems to be raising. Threat landscape is getting increasingly saturated with malicious intents. Actors need to be adaptable and creative when setting up mechanisms that deter from such conduct.

Nowadays, cyber incidents are no longer isolated events but occur on a daily basis. Responses to these incidents can vary significantly, for example, economic, diplomatic, criminal or *"hacking back"*.[1] Given the increasing frequency of incidents, the issue requires due attention.

The violation of an international obligation *"entails the international responsibility"*[2] of the States. In this context, a State which commits an unlawful act from an international perspective and whose liability has been established under the rules of

[1] CODREANU, C. Beyond Short-Lived Responses to Malicious Cyber Operations: The UN GGE and OEWG Processes. *Europolity: Continuity and Change in European Governance* [online]. 2024, Vol. 18, No. 2, pp. 40–41 [cit. 2026-03-07]. Available at: https://doi.org/10.25019/europolity.2024.18.2.2.

[2] International Law Commission. Responsibility of States for Internationally Wrongful Acts. 2001, Art. 1.

international law may be subject to sanctions.[3] The existence of legal framework for sanctions raises the issue of their practical impact.

Given the complexity of situations, that require the use of sanctions mechanisms, it is necessary to moderate expectations of their effectiveness. Expecting a change in the behaviour of an actor targeted by a sanctions regime is quite bold. Historically, only about 10% of actors have changed their behaviour as a result of sanctions.[4] Sanctions should rather be intended to serve as a tool for signalling, that the activities of an actor have crossed a line and it will not stay unanswered. They could also be more useful as a means for negotiating a better position.

For the purposes of this article, the key terminology is briefly clarified. The term *"cyber attack"* is according to the Tallinn Manual *"cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects"*.[5]

The term *"sanctions"* generally refers to policies that restrict trade in between sovereign nations, however their nature does not need to be strictly economic or financial. Overall, they are politically motivated. The role of sanctions becomes significant and is growing. It can be a tool or a means for the policymakers to impose specific norms and behaviour to another actor. Nowadays the term *"sanctions"* is widely used in both legal and political discourse. It is hardly surprising that sanctions are also considered to be an Achilles heel of international law.[6]

International law does not provide specific definitions for the term *"cyber sanctions"*. Nevertheless, through Articles on Responsibility of States for Internationally Wrongful Acts, it reflects the issues of the state responsibility and responses for internationally wrongful acts. The EU has developed more detailed framework specialised for cyber sanctions, within which *"restrictive measures to deter and respond to cyber-attacks with a significant effect"*[7] may be considered as *"cyber sanctions"*.

In this article, the following hypothesis is going to be assessed: *"In the cyber context, the effectiveness of sanctions depends less on their formal legal authority than on institutional flexibility and the ability to respond under conditions of attribution uncertainty,*

---

[3] TROCAN, L. M. Sanctions in Public International Law. In: *Dny práva – 2009 – Days of Law: 3. ročník mezinárodní konference pořádané Právnickou fakultou Masarykovy univerzity – The Third Year of the International Conference Held by Masaryk University, Faculty of Law: sborník příspěvků – the Conference Proceedings* [online]. Brno: Masaryk University, 2009 [cit. 2026-03-07]. Available at: https://www.law.muni.cz/sborniky/dny_prava_2009/files/prispevky/mezin_soud/Trocan_Laura_Magdalena.pdf.

[4] BIERSTEKER, T. *UN Sanctions and Peace Negotiations: Possibilities for Complementarity* [online]. Oslo Forum Papers No. 004. Geneva: Centre for Humanitarian Dialogue, 2015, p. 8 [cit. 2026-03-07]. Available at: https://www.hdcentre.org/wp-content/uploads/2015/02/Oslo-Forum-Paper-UN-sanctions-and-peace-negotiations.pdf.

[5] SCHMITT, M. N. (ed.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017, Rule 92.

[6] ONDŘEJEK, P. Sanctions from the Point of View of (General) Legal Theory. In: ŠTURMA, P. (ed.). *International Sanctions and Human Rights* [online]. Cham: Springer, 2024, pp. 35–52 [cit. 2026-03-07]. Available at: https://doi.org/10.1007/978-3-031-69019-8.

[7] Council of the European Union. Council Regulation (EU) 2019/796 of 17 May 2019 Concerning Restrictive Measures Against Cyber-Attacks Threatening the Union or Its Member States.

which places the European Union in a more operationally effective position than the United Nations."

The topic will be analysed primarily through the lens of public international and European law. The methodology of this article is based on the analysis of available literature, mainly articles regarding international law in cyberspace, but also sanctions in general. The analysis is based in particular on the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), the Charter of the United Nations, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Tallinn Manual), Council Decision (CFSP) 2019/797 and Council Regulation (EU) 2019/796. Secondary sources are used as a complementary support of the analysis.

Due to the fact that cyberspace and by extension, cyber sanctions are a specific topic, it is not a frequently discussed phenomenon. When discussing sanctions in general, they are often assessed through their economic impact. The quantitative data regarding sanctions related to cyberspace is however limited and the effects of sanctions are often not publicly available. In order to avoid potentially misleading data, we will look at the different approaches of EU and UN to sanctions through a comparative analysis, focusing on legal and institutional features.

The article is divided into three main chapters, in each chapter, EU and UN are examined separately. The first chapter deals with legal basis of sanctions mechanisms. The second chapter analyses the application of sanctions mechanisms. The third chapter examines the effectiveness of these mechanisms. The thesis concludes with the final chapter that provides an evaluation of both approaches.

I. LEGAL FRAMEWORK OF SANCTIONS MECHANISM

Cyber sanctions are the means of responding to malicious cyber activities. The decisions about cyber sanctions are not always the most long-winded parts of the process, as they can be imposed to states to which the attacks were attributed. The process of attribution is a lengthy and challenging task, yet necessary, as imposing sanctions without sufficient evidence could only lead to an escalation of the situation.[8]

It is not disputed that international law applies to cyberspace, however, the question regarding the way to apply the traditional international law principles in an abstract domain as cyberspace remains. Not every cyber operation is a breach of international law, therefore malicious activities such as cybercrime or cyber espionage do not necessarily constitute a violation.[9] For the cyber operation to be established as internationally

---

[8] KAPSOKOLI, E. Sanctions and Cyberspace: The Case of the EU's Cyber Sanctions Regime. In: *Proceedings of the 20th European Conference on Cyber Warfare and Security (ECCWS 2021): A Virtual Conference Hosted by University of Chester UK 24th–25th June 2021* [online]. UK: Academic Conferences International Limited Reading, 2021 [cit. 2026-03-07]. Available at: https://doi.org/10.34190/EWS.21.029.

[9] NUREDIN, A. – İNAN, T. Cyber Warfare and International Criminal Law: State Responsibility for Cyber Attacks. In: *International Scientific Conference on AI, Human Rights, Migration, Democracy, and Public Impact: Congress Proceedings* [online]. 2024, pp. 189–201 [cit. 2026-03-07]. Available at: https://doi.org/10.55843/ISC2024conf189n.

wrongful act according to the Rule 14 in Tallinn Manual, the action or omission needs to qualify as *"breach of an international legal obligation applicable to that state"*.[10] A shared understanding on what is objectively considered to be a breach of law would be desirable.[11] As cyber operations continue to grow in sophistication and impact, the international legal community must adapt its frameworks to ensure that states can effectively manage and respond to challenges of the digital age. State conduct in cyberspace lacks effective enforcement, the only reasonable means of regulating seem to be sanctions.

Sanctions in response to cyber operations can, from the perspective of international law, take the form of countermeasures or retorsions. Retorsions are legal acts *per se*, which are defined as acts of unfriendly nature, wrongful in a political sense.[12] Countermeasures are permitted only in cases, where there had been attributable international law violations. They are discussed in the Articles on Responsibility of States for Internationally Wrongful Acts and Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.[13]

In response to cyber attacks, sanctions differ from conventional targeted restrictive measures, since they do not rely on the logic of *"pre-crime"*.[9] Instead of acting on present or future threats, they address a specific past conduct.[14] They constitute a novel sanctions regime, laying the foundations for personalised deterrence with respect to malicious cyber actors and consisting of asset freezes and visa bans.

EU and UN represent two different actors playing a crucial role in cybersecurity governance. Different structures present inevitable differences in their effectiveness. The common denominator is that their power hinges on cooperation.

1. EU

The idea *"global, open, free, stable and secure cyberspace"* has been consistently reflected in EU strategic policy documents.[15] Cyber policy of EU is currently

---

[10] SCHMITT (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, p. 84.

[11] POLI, S. – SOMMARIO, E. The Rationale and the Perils of Failing to Invoke State Responsibility for Cyber-Attacks: The Case of the EU Cyber Sanctions. *German Law Journal* [online]. 2023, Vol. 24, No. 3, pp. 522–536 [cit. 2026-03-07]. Available at: https://doi.org/10.1017/glj.2023.25.

[12] KLUČKA, J. *Medzinárodné právo verejné: všeobecná a osobitná časť* [Public International Law: General and Special Parts]. 4th ed. Bratislava: Wolters Kluwer, 2022.

[13] BOGDANOVA, I. – VASQUEZ CALLO-MÜLLER, M. Unilateral Cyber Sanctions: Between Questioned Legality and Normative Value. *Vanderbilt Journal of Transnational Law* [online]. 2021, Vol. 54, pp. 911–954 [cit. 2026-03-07]. Available at: https://www.researchgate.net/publication/356716815_Unilateral_Cyber_Sanctions_Between_Questioned_Legality_and_Normative_Value.

[14] MIADZVETSKAYA, Y. EU Sanctions in Response to Cyber-Attacks as Crime-Based Emergency Measures. *Computer Law & Security Review* [online]. 2024, Vol. 54, Art. No. 106010 [cit. 2026-03-07]. Available at: https://doi.org/10.1016/j.clsr.2024.106010.

[15] BENDIEK, A. – SCHULZE, M. *Attribution: A Major Challenge for EU Cyber Sanctions* [online]. SWP Research Paper 11. Berlin: Stiftung Wissenschaft und Politik – German Institute for International and Security Affairs, 2021, p. 7 [cit. 2026-03-07]. Available at: https://www.swp-berlin.org/10.18449/2021RP11/#hd-d41750e1025.

based on the EU Cyber Security Strategy 2020–2030.[16] EU is exercising its own autonomous foreign policy competence, which includes sanctioning. Therefore, these measures cannot be considered as countermeasures as outlined by international law, but rather measures, which are autonomous and of a restrictive nature.

In general, EU has an extensive experience with sanctions as a policy instrument. In cybersecurity area, it has created strategies, institutions, as well as policies to ensure secure cyberspace for its Member States. In the EU, sanctions regimes are consistently referred to as restrictive measures, not only in the public communication but also in the legal framework such as treaties and other legal acts.[17]

The EU can enact sanctions against natural and legal persons responsible for (attempted) cyber attacks with significant effects that constitute a threat to the EU and security of its Member States.[18] Sanctions are policy instruments, they do not determine legal liability.

In our case, Article 21 of Treaty on European Union serves as a guideline for foreign and security policy of the EU, as it states the main principles of its action, whilst Article 29 provides a legal basis for Council decisions regarding the Common Foreign and Security Policy (CFSP).[19]

The increasing number of cyber attacks in the EU led to the launch of Cyber Diplomacy Toolbox (CDT) – a framework, but not in a legal sense. It provides EU and Member States with coordinated guidance on how to prevent, respond and deter malicious cyber operations, which includes cyber sanctions. The CDT lowers the threshold between a technical and a political response.[20]

Sanction regime of EU related to cybersecurity is based on Council Decision (CFSP) 2019/797 and Council Regulation (EU) 2019/796. The aim was to create the first horizontal sanction framework independent from geographical and thematical restrictions. This framework gives EU the ability to impose targeted restrictive measures. For the first time it permits EU to impose sanctions against persons or entities, who are responsible for cyber attacks or malicious activities.[21] Before 2019, it was not possible to list individuals responsible for cyber activities on the *"geographical"* sanction list. Geographical sanction regimes didn't include a category for cyber attacks.

---

16 European Commission. Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade, JOIN/2020/18 final. In: *EUR-Lex: Access to European Union Law* [online]. 16. 12. 2020 [cit. 2026-03-07]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020JC0018.

17 Council of the European Union. Why Sanctions. In: *European Council* [online]. 12. 10. 2024 [cit. 2026-03-07]. Available at: https://www.consilium.europa.eu/en/policies/why-sanctions/.

18 MIADZVETSKAYA, *c. d.*

19 Consolidated Version of the Treaty on European Union. *Official Journal of the European Union* [online]. 26. 10. 2012, C 326/15 [cit. 2026-03-07]. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF.

20 Council of the European Union. Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), ST-10474/17 [online]. 19. 6. 2017 [cit. 2026-03-07]. Available at: https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf.

21 KAPSOKOLI, *c. d.*

Council also designates, in an annex, a *"list of natural and legal persons, entities and bodies"*, or in other words, those subject to sanctions.[22] Council decisions must be taken unanimously and list reviewed on an annual basis. The regulation was supported mainly by the UK and Netherlands, as the countries with high exposure to early significant attacks (Parliament and OPCW cyber attack[23]). The importance of the regulation is mainly due to its binding legal nature. It presents an enormous shift from CDT.

The regulation specifies the characteristics that the attack must meet. There are sanctions against critical infrastructure, essential services, critical state functions, storage or processing of classified information, government emergency response teams, EU institutions and CSDP missions and operations.[24]

In 2023, there was a revision of Cyber Diplomacy Toolbox, which led to stronger focus of EU cyber politics on persistent threat actors, information sharing and collaboration, and also to *"exploring the possibility to use sectoral sanctions and* […] *possibility to amend or extend the EU cyber sanctions regime".*[25]

2. UN

The fact that international law is applicable to cyber conduct is virtually undisputed. Firstly, cyber operations in connection with international law were discussed within academic discourse.[26] One of the first cyber operations that coined the term *"cyber warfare"* was Estonia 2007 cyber attack. It was the first time when one state actor attacked another in order to interfere with the domestic and foreign policy.[27] It could be seen as a turning point, from which cyber attacks came to be considered as an issue of international law or at least attracted increasing attention. The research project regarding cyber aspects and international law was launched in 2009 by NATO Cooperative Cyber Defence Centre of Excellence.[28] The creation of the centre was in order to enhance cyber defence of NATO.[29] The research project included experts whose work resulted in the creation of Tallinn Manual on the International Law Applicable to Cyber Warfare. The Tallinn Manual 2.0 on the International Law applicable to

---

22 Council of the European Union. Council Regulation (EU) 2019/796 of 17 May 2019…

23 Dutch Authorities Brief World Chemical Weapons Watchdog on Alleged Russian Cyber Attack. In: *United Nations: UN News* [online]. 4. 10. 2018 [cit. 2026-03-07]. Available at: https://news.un.org/en/story/2018/10/1022262.

24 KAPSOKOLI, *c. d.*

25 Council of the European Union. Revised Implementing Guidelines of the Cyber Diplomacy Toolbox, ST 10289/23 [online]. 8. 6. 2023 [cit. 2026-03-07]. Available at: https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf.

26 SCHMITT, M. N. The Law of Cyber Warfare: Quo Vadis? *Stanford Law & Policy Review* [online]. 2014, Vol. 25, No. 2, pp. 269–270 [cit. 2026-03-07]. Available at: https://law.stanford.edu/publications/law-cyber-warfare-quo-vadis/.

27 CODREANU, *c. d.*

28 SCHMITT, *The Law of Cyber Warfare…*, pp. 269–299.

29 BENATAR, M. – GOMBEER, K. Cyber Sanctions: Exploring a Blind Spot in the Current Legal Debate. In: KRISCH, N. – MÄLKSOO, L. – PROST, M. (eds.). *ESIL Conference Paper Series* [online]. 2011, Vol. 1, No. 1 [cit. 2026-03-07]. Available at: https://www.researchgate.net/publication/228148961_Cyber_Sanctions_Exploring_a_Blind_Spot_in_the_Current_Legal_Debate.

Cyber Operation expands the scope of its predecessor. It systematically clarifies how international law applies to cyberspace.[30] Version 3.0 of the Tallinn Manual is in the process of making.

The prohibition of the threat of force or use of force stated in the Article 2 (4) UN Charter is a peremptory norm (jus cogens). For cyber operation to be a violation of this Article, the Tallinn Manual provides a basis. It states that *"cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force"*.[31]

The threshold can be simplified to so-called *"scale and effects"*, which need to be taken into consideration and be comparable to operations of a kinetic nature.[32] Similarly the same *"scale and effects"* assessment applies to the Article 51 of the UN Charter, regarding the right to individual or collective self-defence, *"cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence"*.[33]

At the institutional level of the UN, there are two ongoing processes, known as working groups. UN dynamics are based on consensus building rather than enforcement. These working groups are essential even though they do not operationalise sanctions. However, they focus on cyber governance, such as normative preparation from UN Security Council. UN Group of Governmental Experts (GGE), created in 2004, presented its most recent report in 2021. In its reports it repeatedly affirms the existence and relevance of UN Charter and the responsibility of states in cyberspace.[34] GGE has a mostly normative function and the relevance for sanctions lies in the affirmation of the existence of international law norms applicable for cyberspace. Therefore, if violated, sanctions can be imposed. The reports are not legally binding, but they still sustain the legal relevance, as the UN Security Council does not have a specific cyber sanctions regime, but remains central to cyber governance through GGE.

GGE advantage also lies in the creation of normative bridge, because EU decisions regarding sanctions seem to be in consistency with international law as well as supporting the UN. Every mandate of GGE working formation was affected by events occurring in that specific period of time. As the most influential cyber operations, the following could be mentioned: attacks in Estonia, Georgia, Stuxnet, Shamoon in Saudi Arabia, US presidential election interference in 2016, NotPetya, WannaCry, SolarWinds, and others.[35]

The second UN group, Open-Ended Working Group (OEWG), established in 2019, was formed to balance the GGE. Throughout its formation, it became more inclusive of all UN Member States and far more influential. Nature of stakeholders is different in

---

30 SCHMITT, *The Law of Cyber Warfare…*, pp. 269–299.

31 SCHMITT (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 69.

32 POLI – SOMMARIO, *c. d.*

33 SCHMITT (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 71.

34 United Nations: General Assembly. Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security [online]. 2021 [cit. 2026-03-07]. Available at: https://dig.watch/wp-content/uploads/2022/08/UN-GGE-Report-2021.pdf.

35 CODREANU, *c. d.*

those groups, OEWG includes also non-government actors.[36] In order to gain support for Russian and Chinese proposals, it was actually Russia that proposed the creation of the OEWG, formed to prevent deadlock, that was experienced in GGE group.[37]

The OEWG mandate was renewed for the period 2021 to 2025.[38] The Final Report of the OEWG in 2025 successfully adopted the Global Mechanism (United Nations Global Mechanism on developments in the field of ICTs in the context of international security and advancing responsible State behaviour in the use of ICTs)[39]. It is the single-track, permanent intergovernmental platform intended to ensure continuity in UN efforts regarding ICT security.[40] The launch of the Global Mechanism is scheduled for March 2026, marking a milestone for international cybersecurity policy.

The Norms of Responsible State Behaviour in Cyberspace were introduced by GGE and later endorsed by UN General Assembly by Resolution 70/237 (2015). OEWG in its reports added details needed by governments for better understanding and implementation. Although these norms are not binding, they present expectations of international community.[41]

UN Framework of Responsible Behaviour in Cyberspace consists of eleven voluntary norms, as it might be seen from a normative point of view. It also includes other matters: recognition of applicability of international law in cyberspace, set of confidence building measures and commitment to coordinated cyber capacity building.[42]

EU is very much on the same note with the idea of responsible behaviour of states in cyberspace. In 2024, Council approved the Declaration on a Common Understanding of International Law in Cyberspace. This also marks the first time when EU and its Member States adopted a declaration regarding cyberspace. It is one of the efforts of OEWG and it reaffirms that EU has a full commitment to the implementation of the UN framework of responsible state behaviour in cyberspace.[43]

---

36 BOGDANOVA – VASQUEZ CALLO-MÜLLER, *c. d.*

37 CODREANU, *c. d.*

38 LAHMANN, H. State Behaviour in Cyberspace: Normative Development and Points of Contention. *Zeitschrift für Außen- und Sicherheitspolitik* [online]. 2023, Vol. 16, pp. 31–41 [cit. 2026-03-07]. Available at: https://link.springer.com/article/10.1007/s12399-023-00939-7?utm_source=researchgate.net&utm_medium=article.

39 United Nations: General Assembly. Developments in the Field of Information and Telecommunications in the Context of International Security, A/80/257 [online]. 24. 7. 2025 [cit. 2026-03-07]. Available at: https://docs.un.org/en/A/80/257.

40 KULESZA, J. Lecture at Cyberdiplomacy Advanced Course (European Security and Defence College).

41 HOGEVEEN, B. *The UN Norms of Responsible State Behaviour in Cyberspace* [online]. The Australian Strategic Policy Institute Limited, 2022, p. 8 [cit. 2026-03-07]. Available at: https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf.

42 Ibid.

43 Council of the European Union. Cyberspace: Council Approves Declaration to Promote Common Understanding of Application of International Law. In: *European Council* [online]. 18. 11. 2024 [cit. 2026-03-07]. Available at: https://www.consilium.europa.eu/en/press/press-releases/2024/11/18/cyberspace-council-approves-declaration-to-promote-common-understanding-of-application-of-international-law/.

II. APPLICATION OF SANCTION MECHANISMS

Why are sanctions even applied in the first place? From the strategic point of view, it is the concept called cyber deterrence. Due to the problematic attribution in cyberspace and other issues, it might not be as effective as the concept was supposed to be.[44] For holding the state accountable followed by the imposing of sanctions, under the international law, the cyber operation must be attributed.

1. EU

On an EU level, attribution is a sovereign act by the EU Member States, whose capabilities differ. It remains within the competence of individual states. EU itself coordinates and distributes evidence and intelligence. Attribution is quite a challenge for the conduct of cyber diplomacy as well as cyber sanctions regime. For imposing sanctions on an EU level, coordinated attribution assessment between Member State and EU must take place, but it does not require formal attribution, invocation of state responsibility.[45]

There is a special agency related to cybersecurity, often considered as the heart of EU cybersecurity, European Network and Information Security Agency (ENISA).[46] ENISA doesn't have direct approach to cyber sanctions, but serves as a technical support for attribution. The EU does not attribute cyber operations to states as a matter of international responsibility, it is reserved to the individual Member States.[47]

For the application of this rule, it is necessary to be clear about what is considered to be an attack. Under Slovak conditions, we could use a term *"attack"* for an action that endangers availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or related services provided or accessed through networks and information systems.[48] The Council Decision 2019/797 in the third paragraph of Article 1 states that cyber attacks are actions involving *"a) access to information systems; b) information system interference; c) data interference; or d) data interception"*.[49] In order to fall within the scope of the EU restrictive measures, the attack needs to be carried out from outside of the EU.[50]

---

44 BOGDANOVA – VASQUEZ CALLO-MÜLLER, *c. d.*

45 BENDIEK – SCHULZE, *c. d.*, p. 8.

46 BENATAR – GOMBEER, *c. d.*

47 POLI – SOMMARIO, *c. d.*

48 *Krátky terminologický slovník* [A Short Terminology Glossary]. Bratislava: Národné bezpečnostné analytické centrum, 2021.

49 Council of the European Union. Council Decision (CFSP) 2019/797 of 17 May 2019 Concerning Restrictive Measures Against Cyber-Attacks Threatening the Union or Its Member States, ST/7299/2019/INIT. In: *EUR-Lex: Access to European Union Law* [online]. 17. 5. 2019 [cit. 2026-03-07]. Available at: https://eur-lex.europa.eu/eli/dec/2019/797/oj/eng.

50 POLI – SOMMARIO, *c. d.*

EU has more than 50 sanctions programmes in place.[51] Success of sanctioning depends on the reliable evidence, its formal correctness and secure information handling. Apart from the US, the EU is the only international actor that has proposed and applied cyber sanctions as a policy option in order to deal with cybersecurity issues.[52] Cyber sanctions regime is first of its kind, horizontal, enabling targeted sanctions to specific cyber attacks rather than specific state geographically.

In 2020, the first year of existence of cyber sanctions regime brought also the first applied sanctions, as they were not applied immediately after the creation of this regime. These sanctions, associated with the Russian, North Korean and Chinese government,[53] were in the form of travel bans and asset freezes against responsible persons and entities for multiple attacks targeted against the EU and its Member States.[54] The attribution to individuals and entities was supported by EU partners, but negatively perceived by attackers.[55] In this first package, there were twelve entities sanctioned. It is a clear demonstration of EU ability to react to cyber activities.

The second package of cyber sanctions was imposed in 2024. It included six individuals and reflected the increasing trend of ransomware, which became a tool widely used for heightening of geopolitical tensions.[56]

In January of 2025, the third cyber sanctions package was agreed upon, it included three entities.[57] It shows a shift to attacks connected with intelligence gathering and espionage, that present a direct threat with significant effect for Member States.

The whole process of imposing sanctions lasts relatively long time, as it consists of many phases. Member States need to prepare a proposal for entities to be included in the sanction list. It includes gathering of evidence and subsequently, a consultation period. After the comments, proposal is discussed in the working groups. Just for illustration, the whole process could last about two months.[58] In the whole proposal, the essential part is an evidence pack, that must include not only intelligence information, but also information gathered by OSINT.

---

51 EU Sanctions: A Key Foreign and Security Policy Instrument. In: *Think Thank: European Parliament* [online]. 12. 4. 2024 [cit. 2026-03-07]. Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2024)760416.

52 KAPSOKOLI, *c. d.*

53 BENDIEK – SCHULZE, *c. d.*, p. 5.

54 Ibid.

55 KAPSOKOLI, *c. d.*

56 REPA, R. *Seminary to Sanctions Politics of EU Regarding Cyber Issues*. October 2025.

57 Council of the European Union. Council Implementing Regulation (EU) 2025/173 of 27 January 2025 Implementing Regulation (EU) 2019/796 Concerning Restrictive Measures Against Cyber-Attacks Threatening the Union or Its Member States, ST/5130/2025/INIT. In: *EUR-Lex: Access to European Union Law* [online]. 27. 1. 2025 [cit. 2026-03-07]. Available at: https://eur-lex.europa.eu/eli/reg_impl/2025/173/oj/eng.

58 REPA, *c. d.*

2. UN

In the UN system, the main responsibility for international peace and security rests with the Security Council. The same applies for cyberspace and cybersecurity.[59]

Sanctions at the UN level are used as a tool for maintaining peace and security. They are adopted exclusively by the Security Council under the Chapter VII of the UN Charter, which provides a legal basis for binding measures. The binding force of Security Council decisions is derived from Article 25 of the UN Charter, through which UN Member States *"agree to accept and carry out the decisions"* of the Security Council.[60] Despite of that, activities of the Security Council are often blocked mainly due to its composition and veto power of permanent members.

For Security Council to invoke its powers in Chapter VII, criteria within Article 39 of the UN Charter must be fulfilled. However, the situation needs to be qualified as *"threat to the peace, breach of the peace, or act of aggression"*. If the political will is absent, it is unlikely that a political decision – qualification will be made. Without the qualification, SC lacks the legal basis for further response. The response to Estonia cyber attacks in 2007 can be an example when UN did not take any formal steps or institutional sanctions.[61]

The threshold for action is intentionally high. Is there some connection though? We might assume so. Security Council actions are reserved for situations, that could present a threat to international peace and security. In that case, are cyber attacks not considered to be threats to the international order? If yes, why are they not qualified as an independent category of threats warranting sanctions? As there are many determinants whether cyber attacks currently pose high risks to international peace, they are not legally established as threats. The workflow of Security Council is shaped by political consensus among permanent members, who are one of the most active players in the cyberspace.

There is no specific cyber sanctions regime at the UN level and sanctions are usually thought of as a last resort. Cyber operations are considered to be one of the tools used within hybrid threats.[62] Responses to them are addressed though the international law, specifically rules on the state responsibility.

As discussed in the previous chapter, the UN approach to cyberspace is far more preventive and normative as UN focuses on norm development rather than its enforcement. In this context, the use of countermeasures to cyber attacks is still subject to

---

[59] MELZER, N. *Cyberwarfare and International Law* [online]. Geneva: United Nations Institute for Disarmament Research, 2011 [cit. 2025-12-19]. Available at: https://unidir.org/files/publication/pdfs/cyberwarfare-and-international-law-382.pdf.

[60] MOISEIENKO, A. Crime and Sanctions: Beyond Sanctions as a Foreign Policy Tool. *German Law Journal* [online]. 2024, Vol. 25, No. 1, pp. 17–47 [cit. 2026-03-07]. Available at: https://doi.org/10.1017/glj.2023.103; United Nations Charter (full text). In: *United Nations* [online]. [cit. 2026-03-07]. Available at: https://www.un.org/en/about-us/un-charter/full-text.

[61] BENATAR – GOMBEER, *c. d.*

[62] European Commission. Joint Framework on Countering Hybrid Threats: A European Union response, JOIN(2016) 18 final. In: *EUR-Lex: Access to European Union Law* [online]. 6. 4. 2016 [cit. 2026-03-07]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018.

debate. Traditionally only injured states can react and use countermeasures. Emerging trends are of opinion that also a state that has not been directly affected, especially in the cyber context, can take the form of collective countermeasures.[63] Countermeasures, as defined in Chapter II of ARSIWA, are actions that would normally violate the international law, but are used by injured state as a response to wrongful act. The requirements for countermeasures to be justified include: temporary nature, purpose, reversibility, proportionality and refraining from fundamental obligations.[64] The application of these principles is further discussed in the Tallinn Manual.[65]

III. THE EFFECTIVENESS OF SANCTIONS MECHANISMS

Attribution of cyber operations is a key element when responding to malicious cyber activities. However, does it alone provide a sufficient deterring effect to prevent future attacks or must sanction mechanisms be adopted?[66]

The effectiveness of sanction mechanisms is a complex topic, studied for a very long period of time. The indicators we could take into consideration would definitely include policy goals and security. The imposition of sanctions in response to cyber attacks seems not to have led for the target states. The key outcome of sanctions is the change in the target's behaviour, but there is an absence of any evidential signs of that kind.

In the evaluation of effectiveness, it might be beneficial to consider available alternatives. It is important to compare sanctions with other available tools and maintain proportionality and their multilateral nature. Sanctions should be used in combination with other tools, such as diplomacy, law enforcement, dialogue and cooperation.[67] After all, cyber sanctions might not be that effective without strong cooperation.[68] If these conditions are not met, sanctions might have adversary effects and the credibility of those, who implemented the sanctions is likely to be weakened.[69]

The brief look at the topic of sanctions as such, could suggest that they are not effective, because from the time when the first cyber related sanctions were imposed (regardless whether speaking about EU or UN) there has not been a decrease in these malicious acts. Despite the sanctions being always considered as economic matters, they are a political issue. The assessment of effectiveness should not be based solely on numbers. To be more objective, we have decided to pick some of the determinants to be able to create less biased comparison, which are discussed in the next chapter. It is also worthwhile to mention, that the effectiveness of sanctions overall depends on their

---

63 International Law Commission, *c. d.*

64 Ibid.

65 MARTYNOVA, E. Collective Countermeasures in Response to Cyber Operations Under International Law. *Legal Issues in the Digital Age* [online]. 2024, Vol. 5, No. 3, pp. 103–128 [cit. 2026-03-07]. Available at: https://doi.org/10.17323/2713-2749.2024.3.103.128.

66 CODREANU, *c. d.*

67 KAPSOKOLI, *c. d.*

68 Ibid.

69 Ibid.

intended objectives. At the same time, the targeted actors can diversify their policies regarding the sectors that are targeted (e.g. diversify their production, import from other sources, etc.) and thereby become more independent and minimise the impact of sanctions.[70] In light of these considerations, the subchapters that follow examine selected aspects of effectiveness from the point of EU and UN.

1. EU

Legal and binding nature

Responses to cyber attacks do not fall within an exclusive EU competence, therefore Member States can react individually. From the point of effectiveness, coordinated reaction is usually more advantageous. Sanctions that are imposed as a common reaction through EU have regional binding force and are accompanied by broader impact.[71]

EU sanctions are based on a doctrine of behaviour change, they target entities and individuals in non-EU countries with the intent of bringing about a change in policies or actions.[72] As they take form of asset freezes and visa bans, they are deprived of punitive purpose.[73] The EU cyber sanctions framework further establishes detailed criteria, under which restrictive measures may be imposed.[74]

The binding nature of EU cyber sanctions stems from the legal documents through which they are adopted. Once Council adopts decisions and implements regulations, they become binding and apply across EU Member States.[75]

Responsiveness and institutional effectiveness

The sanctions are reserved only for attacks, which are major because their adoption and implementation involve significant political, legal and administrative costs. However, they can be still considered as quite fast and flexible reactions. Regulation 2019/796 also states, that cyber sanctions fulfil not only a reactive function, but also a preventive one, as they discourage from similar conduct in the future.

The reaction time depends, in addition on the approach of the Member States. If it was common position, it would be ideal, but in many cases, EU needs to overcome different national approaches.[76]

Moreover, sanctions in regard to cyber operations have a signalling function. According to the research by Targeted Sanctions Consortium, in general, sanctions with

---

70 Ibid.
71 POLI – SOMMARIO, *c. d.*
72 MOISEIENKO, *c. d.*
73 POLI – SOMMARIO, *c. d.*
74 BOGDANOVA – VASQUEZ CALLO-MÜLLER, *c. d.*
75 BENDIEK – SCHULZE, *c. d.*
76 BOGDANOVA – VASQUEZ CALLO-MÜLLER, *c. d.*

intent to signal or constrain are three times more effective than those intended to change behaviour.[77]

The deficiencies that undermine the effectiveness of sanctions include already mentioned attribution, which is interconnected with the lack of reliable evidence.[78]

Proportionality and appropriateness of measures

Restrictive measures under EU are designed to avoid disproportions in consequences without excessive effects. It comes from the nature of EU cyber sanctions that they are targeted, aimed at individuals and groups. The coercive effect stemming from the sanctions is quite limited, as they are targeted to individuals. In their case, there is not a high probability that it could affect states when it is imposed on number of individuals. If the sanctioned are deprived of resources, they have higher chance of discontinuing malicious activities.

Horizontal regime of cyber sanctions is quite flexible as it is not limited to any geographic region. The response to attack can be created also by other elements from CDT, alongside sanctions. It ensures that response is adjusted to the severity of attack.[79]

Despite the need of consensus among Member States where only unanimous vote leads to adoption of sanctions, EU cyber sanctions regime presents a good balance of effectiveness with proportionality. This regime is quite flexible, but adoption process still generates considerable delays.

Normative contribution to the international order

The EU appears in the *"international arena"* as an actor of cyber diplomacy. An interesting outcome is that EU imposes cyber sanctions but does not trigger rules on international legal responsibility.[80] Sanctions are considered as a form of *"normative power"*.[81]

Despite the fact that EU has in general many sanctions regimes, cyber related sanctions are very specific and there is not an absolute match in regards to the approaches to cybersecurity. Other problems could be a lacking technical capacity or intelligence to attribute attacks or disclosure of information that could be very useful for attackers in their possible future attack.

The requirement of unanimity may be problematic in Council Decisions adopting, particularly regarding the annex. Sanctions are not imposed very often due to the fact that Member States with ties to states from which malicious activities originate often consider the imposition of sanctions in a political way.

---

77 RUSINOVA, V. – MARTYNOVA, E. Fighting Cyber Attacks with Sanctions: Digital Threats, Economic Responses. *Israel Law Review* [online]. 2024, Vol. 57, No. 1, pp. 135–174 [cit. 2026-03-07]. Available at: https://doi.org/10.1017/S0021223722000255.

78 BOGDANOVA – VASQUEZ CALLO-MÜLLER, *c. d.*

79 BENDIEK – SCHULZE, *c. d.*, pp. 16–18.

80 POLI – SOMMARIO, *c. d.*

81 BALAKHONOVA, S. Cyber Sanctions as a Tool of Competition in Global Cyberspace. *Journal of International Analytics* [online]. 2023, Vol. 14, No. 1, pp. 52–71 [cit. 2026-03-07]. Available at: https://doi.org/10.46272/2587-8476-2023-14-1-52-71.

Older study from 2019, introduces ten rules that policymakers should follow to ensure that sanctions will be as much effective as possible. All issues are of significant importance, as there are points such as strategic communication, cooperation with partners but also engagement with private sector.[82]

2. UN

Legal and binding nature

The UN sanctions are universally applicable, as they derive their authority from the UN Charter, namely Chapter VII. They are legally binding on all UN Member States. Potentially they have global reach and greater impact than EU cyber sanctions regime which is of regional nature.

As it was discussed above, a specific sanctions regime related to cyberspace does not exist, cyber sanctions do not create a separate category, nonetheless UN Security Council resolutions in this regard do have binding effects. Overall UN possesses binding authority, but not through dedicated cyber sanctions regime.

Responsiveness and institutional effectiveness

The whole process of adopting sanctions within UN Security Council tends to be lengthy as Security Council is more focused on traditional threats. Even cyber activities are often taken as a part of wider narratives.

Security Council is constrained by veto power of its permanent members, as sanctions need to be accepted by permanent members. These tend to be allied with the perpetrators of the attack or even carry out similar attacks themselves. Achieving agreement is rather difficult and slow, but on the other hand legally authoritative. The effectiveness of imposed sanctions is interconnected with the attribution problem through the lack of reliable evidence that can create an obstruction of sanction adoption.[83]

Proportionality and appropriateness of measures

As for the proportionality, Security Council measures have undoubtedly wider reach. Sanctions adopted under the Chapter VII UN Charter are binding on all UN Member States and therefore their consequences might be more extensive which could increase the effectiveness. As noted above, UN has not created dedicated cyber sanctions regime, which leads to an absence of criteria for determining the appropriate sanctions. This stems from the legal nature, UN sanctions are more relevant to general matters, what is reflected in the extent of sanctions, lacking specific cyber tools. The appropriateness is therefore questionable.

---

[82] PAWLAK, P. – BIERSTEKER, T. (eds.). *Guardian of the Galaxy: EU Cyber Sanctions and Norms in Cyberspace* [online]. Institute for Security Studies, 2019, pp. 15–18 [cit. 2026-03-07]. Available at: https://www.iss.europa.eu/sites/default/files/EUISSFiles/cp155.pdf.

[83] BOGDANOVA – VASQUEZ CALLO-MÜLLER, *c. d.*

Normative contribution to the international order

In comparison to the EU, the basis of UN contribution lies in its normative element. Cyberspace is addressed mainly through mechanisms such as the UN Groups, GGE and OEWG.

The UN has significantly contributed to the framework governing state behaviour in cyberspace. Moreover, it has clarified how international law applies to cyberspace. The fact that the Security Council deals with matters that include cyber issues, even though it does not deal with a specific type of sanctions, only confirms that international law is applicable to the fifth domain. As the whole contribution of UN shifts from coercive to normative, UN effectiveness cannot be measured through sanctions.

CONCLUSION

If we were to think about where sanctions originate, we would come to the true essence of international law. As it was created at a time when a cyber domain was unthinkable, it is of the utmost importance, that it reflects these new dynamics. The same applies to sanctions. States recognise the need to take appropriate measures to secure cyberspace, and sanctions are one of the tools to do so.

The effectiveness of cyber sanctions is not measured by the ability to stop attacks altogether, but rather as a strategic instrument that can be used in contrast to traditional tools. Despite the limited effectivity of cyber sanctions, they cannot be labelled as unsuccessful.

Sanctions are generally very interesting phenomena, as V. A. Silaeva concludes in his work that the effectiveness of international sanctions remains one of the most contested topics in political science. Every case is different as it has its unique mix of factors that affect their efficiency.[84]

Even if there are some changes, for which sanctions could take accountability, it is not truly possible to measure their effectiveness. Usually there are also other means used in combination with sanctions, that could create a deterring effect.

The hypothesis is confirmed, in the cyber context the decisive element is the ability to respond in a flexible way. The importance of legal authority cannot be questioned, but the thresholds are currently high, so it presents a challenge to fulfil the criteria. Therefore, EU seems to be in a more effective position than UN.

The importance of coordinated and legally precise approach to the creation of sanctions regimes is unquestionable. The real question is, how successfully are we going to do so?

Mgr. Petra Lukačovičová
Pan-European University, Faculty of Law
petra.lukacovicova@paneurouni.com

[84] SILAEVA, V. Effectiveness of Sanctions in International Politics. *MGIMO Review of International Relations* [online]. 2021, Vol. 14, No. 4, pp. 136–153 [cit. 2026-03-07]. Available at: https://doi.org/10.24833/2071-8160-2021-4-79-136-153.