UDK 004.738.5:342.7(4-67EU)
Review article

THE COMPATIBILITY OF RESTRICTIVE MEASURES REGARDING CYBERATTACKS WITH THE CHARTER OF FUNDAMENTAL RIGHTS OF THE EU

Eimys Ortiz-Hernández, PhD, Serra Húnter Tenure-Eligible Lecturer of Public International Law and International Relations
University of Lleida
Jaume II, 73., 25001, Lleida, Spain
eimys.ortiz@udl.cat

ABSTRACT

The realm of cyberspace presents a landscape of both promise and peril, spanning economic domains to matters of security. In response, the EU has diligently crafted a comprehensive cybersecurity framework, rooted in cyber diplomacy, to mitigate and counter cyber disruptions and threats. This work embarks on an exploration of the legal underpinnings of restrictive measures or sanctions as outlined in Council Decision 2019/797 and Council Regulation 2019/796. Through a thorough analysis of this framework, the paper scrutinizes the compatibility of unilateral cyber sanctions with the fundamental rights enshrined in the Charter of Fundamental Rights of the EU. It underscores the imperative of clear and unambiguous legislation in upholding due process, safeguarding the rule of law, and preserving the core values of the EU.

Keywords: *Common Foreign and Security Policy, Court of Justice of the EU, cyber sanctions, fundamental rights, judicial review, restrictive measures*

1. INTRODUCTION

In the midst of spring 2022, the Council of the European Union (hereinafter referred to as the Council) resolved to extend until May 18, 2025, the restrictive measures designed to address the threats posed by cyberattacks within the organization and its Member States.[1] This framework empowers the European Union (EU) to enforce targeted restrictive measures against individuals and/or entities implicated in cyberattacks originating beyond the Union's borders, which have

[1] Council of the EU, *Cyber-attacks: Council extends sanctions regime until 18 May 2025*, press release, 16.05.2022, [https://www.consilium.europa.eu/en/press/press-releases/2022/05/16/cyber-attacks-council-extends-sanctions-regime-until-18-may-2025/], Accessed 10 April 2024.

caused or possess the potential to cause substantial disruptions to cybersecurity, thus posing a threat to its own stability and security. Moreover, aligned with the objectives of the Common Foreign and Security Policy (CFSP), there exists the avenue to counter such nefarious activities by imposing sanctions, provided the attack is directed towards third States or international organizations. Presently, eight individuals and four entities are under the purview of restrictive measures, including travel bans to the EU territory and/or asset freezes.[2]

The EU's commitment to transnational cooperation regarding restrictive measures is rooted in Brussels' imperative to firmly oppose cyberattacks. Consequently, it decided to provide itself with specific instruments to be activated when necessary.[3] In light of the escalating quantity and sophistication of cyberattacks, the necessity for cyber deterrence tools was acknowledged.[4] It is worth noting that the European regime was not fortuitous but rather, in a way, the culmination of efforts that began to take shape some years earlier, specifically in 2013. At that time, the Cybersecurity Strategy was launched -updated in 2020- emphasizing the importance of achieving greater coordination within the Union through a coherent international cyber policy.[5] The EU Cyber Defence Policy Framework, adopted in 2014 and revised in 2018, reiterated cybersecurity as a priority of the EU's Global Strategy on Foreign and Security Policy[6], emphasizing the necessity to strengthen the Union as a "security community".[7] In light of these circumstances, it was crucial to supplement the EU's existing instruments, such as the cybersecurity regulation and the directives on network and information systems security, with a joint diplomatic approach, as emphasized by the 2015 Cyber Diplomacy Conclusions, which insisted on the essential nature of formulating a comprehensive action plan

---

2 Council Regulation 2019/796/EU concerning restrictive measures against cyber-attacks threatening the Union or its Member States [2019] OJ L129 I/1.

3 Borrell, J., *Cyber sanctions: time to act*, 30.07.2020, [https://www.eeas.europa.eu/eeas/cyber-sanctions-time-act_en], Accessed 10 April 2024.

4 Arteaga, F., *Sanciones contra los ciberataques: la UE enseña las uñas*, Real Instituto Elcano, Comentario Elcano 19/2019, 11.06.2019, [https://media.realinstitutoelcano.org/wp-content/uploads/2021/11/comentario-arteaga-sanciones-contra-los-ciberataques-la-ue-ensena-las-unas.pdf], Accessed 10 April 2024.

5 Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Cybersecurity Strategy of the EU: an open, safe and secure cyberspace*, JOIN(2013)1 final, Brussels, 07.02.2013. Joint communication to the European Parliament and the Council, *The EU's cybersecurity strategy for the digital decade*, JOIN(2020) 18 final, Brussels, 16.12.2020.

6 European Commission, *A global strategy for the European Union's Foreign and Security Policy*, 2016, [https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf], Accessed 10 April 2024.

7 European Council, *EU Cyber Defence Policy Framework*, 18.11.2014, 15585/14. European Council, *EU cyber defence policy framework (2018 update),* 19.11.2018, 14413/18.

covering accountability for illicit activities.[8] The Council's work continued, and thus, in June 2017, it adopted a set of cyber diplomacy instruments known as the EU Cyber Diplomacy Toolbox.[9] As autumn progressed, the Political and Security Committee approved the implementation guidelines for this set of instruments, addressing five categories of measures, including restrictive measures. With the framework in the making and little time to bolster it, the Union had to face the attacks of WannaCry and NotPetya.[10] Thus, on May 17, 2019, Decision (CFSP) 2019/797 and Regulation (EU) 2019/796 were ratified, both pertaining to restrictive measures against cyberattacks posing a threat to the Union or its Member States. Both legislative frameworks included a blank annex intended for the listing of recipients of the measures, which was expeditiously completed. Subsequently, in July 2020, the initial punitive measures were sanctioned against individuals and corporate entities of Chinese, Russian, and North Korean citizenship, in accordance with a distinctive and intricate regulatory framework.[11]

In essence, the legal framework, predicated on the allocation of competences between Member States and the Union, encompasses the identification of recipients, the nature and victims of cyberattacks, the modalities and scope of restrictive measures, as well as the stipulated safeguards, controls, and legal assurances to ensure the conformity to law of measures enacted by the Council.[12] However, despite Brussels' advocated safeguarding process, what would happen if an individual or entity subject to the described restrictive measures challenged their compatibility with the EU Charter of Fundamental Rights (ECFR)? Which fundamental rights could potentially be undermined by the imposition of sanctions in the context of combating cyber threats? If ambiguity or obscurity were to characterize the future legal response, the effectiveness of the Union's purpose would be eroded. Hence, it

---

8 Council Conclusions on Cyber Diplomacy, Brussels, 11.02.2015.

9 Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), 19.06.2017. Vid., Kasper, A.; Osula, A.M.; Molnár, A, *EU cybersecurity and cyber diplomacy,* Revista d'internet, dret i política, Dossier "Europe facing the digital challenge: obstacles and solutions", No. 34, December, 2012, pp. 1-15; Miadzvetskaya, Y.; Wessel, Ramses A., *The externalization of the EU's cybersecurity regime: the cyber diplomacy toolbox*, European Papers, Vol. 7, No. 1, 2022, pp. 413-438; Moret, E.; Pawlak, P., *The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?*, European Union Institute for Security Studies (EUISS), Brief Issue No. 24, 2017, [https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/EUISS-Brief_24_Cyber_sanctions.pdf] Accessed 10 April 2024.

10 Council conclusions on malicious cyber activities, 16.04.2018, 7925/18.

11 Concerning EU cyber-sanctions *vid.,* [https://www.sanctionsmap.eu/#/main/details/47/?search=%7B%22value%22:%22%22,%22searchType%22:%7B%7D%7D], Accessed 10 April 2024.

12 Robles Carrillo, M., *Sanciones contra ciberataques: la acción de Unión Europea*, Documento de Opinión IEEE 143/2020, [http://www.ieee.es/Galerias/fichero/docs_opinion/2020/DIEEEO143_2020MARROB_ciberUE.pdf], Accessed 10 April 2024.

is worth conducting an analysis of the current legal framework to assess the consistency of the system with the rule of law that the EU upholds as an intrinsic value.

2. LEGAL REGIME ANALYSIS PERTAINING TO THE IMPOSITION OF SANCTIONS AGAINST CYBERATTACKS

Initially, European sanctions practices emerged in response to serious violations of international law, primarily targeting third States.[13] However, the scope later expanded to include the possibility of imposing sanctions on individuals and/or legal entities, aligning with mandates issued by the United Nations Security Council in the aftermath of September 11th.[14] Thus, recourse to primary law becomes imperative to grasp the nuances of the system itself. Article 215 of the TFEU is crafted to reconcile the competences vested in the EU with those retained by Member States in the realm of foreign policy when imposing sanctions on third parties. Under this provision, when a decision is adopted within the framework of the CFSP foreseeing the interruption or reduction, total or partial, of economic and financial relations with one or more third countries or against individuals or legal entities, groups, or non-state entities, the Council shall adopt the necessary measures. Hence, two distinct legal acts with separate procedures are necessitated, albeit both originating from the Council.[15] Accordingly, while article 24 of the TEU mandates unanimity for decisions within the CFSP, article 215 of the TFEU requires qualified majority voting.

Considering these intricacies, the legal framework governing sanctions imposed within the EU framework against malicious activities in cyberspace is delineated by the 2019 Decision and Regulation, which establish the overarching normative framework. Subsequent implementing Decisions and Regulations, adopted in 2020, 2021, 2022, and 2023 respectively, serve to organize the list of individuals, legal entities, entities, and organisms, as well as cyberattacks, targeted by these measures. Additionally, they fulfil the obligation of annual review or adaptation to evolving legislative circumstances. It becomes evident, thus, that the examination

---

13 Hörbelt, C., *A comparative study: where and why does the EU impose sanctions*, Revista Unisci/Unisci Journal, No. 43, January 2017, pp. 53-71.

14 Pawlak, P., *The EU's Role on Shaping the Cyber Regime Complex*, European Foreign Affairs Review Vol. 24, No. 2, 2019, pp. 167-186.

15 Robles Carrillo, M., *op. cit.,* note 12, pp. 5-6. See also, Case C-134/19 P *Bank Refah Kargaran v Council of the European Union* [2020] ECLI:EU:C:2020:793, par. 41 "As the Council itself acknowledges, CFSP Decisions, and the regulations enacted pursuant to Article 215 TFEU to implement them, may not be substantively identical. In particular, as far as natural persons are concerned, restrictions on admission to the territory of the Member States are likely to be included in CFSP Decisions, without necessarily being included in regulations based on Article 215 TFEU […]". See also, Case C-72/15 P *JSC Rosneft Oil Company v. Her Majesty's Treasury and Others*, EU:C:2017:236, par. 89 and 90.

of these instruments facilitates the identification of the key components of the legal framework.

Firstly, within the preamble, the political process underpinning the formulation of both legal instruments is set forth. It is imperative to underscore that the restrictive measures are portrayed as an additional tool in the collective diplomatic response against malicious cyber activities. In essence, authorities sought to achieve two particularly intricate objectives: facilitating the mitigation of immediate threats on the one hand, and shaping the behaviour of potential aggressors in the long term on the other. Thus, the capacity for responsiveness and deterrence would delineate the trajectory to be pursued, while ensuring the preservation of fundamental rights and adherence to the principles enshrined in the ECFR. However, a crucial caveat is introduced, aiming to dissociate the restrictive measures from the attribution of responsibility to a third State for cyberattacks. Alternatively, it is asserted that the application of these measures does not automatically attribute responsibility to the State whose nationality the individual or entity subject to such measures holds. The decision was made in accordance with the principle of sovereignty, whereby States retain the freedom to determine their own stance regarding the attribution of cyberattacks to a third state. Indeed, this provision mitigated the potential political ramifications associated with the issue of third-party State responsibility. Nevertheless, part of the academic discourse has underscored that attribution remains one of the most significant challenges within the established system.[16]

Secondly, the scope of application of the regime is set out, wherein the machinery is activated in response to cyberattacks with significant effects, encompassing attempts that may result in such consequences and also pose an external threat to the

[16] With respect to attribution vid., Bendiek, A.; Schulze, M., *Attribution: a major challenge for EU cyber sanctions*, German Institute for International and Security Affairs, SWP Research Paper No.11, December 2021, Berlin; Delerue, F., *Cyberoperations and international law*, Cambridge University Press, 2020, p. 513; Kijeweski, P.; Jaroszewski, P.; Urbanowicz, J.A.; Armin, J., *The never-ending game of cyberattack attribution*: *Exploring the threats, defenses and research gaps* in: Akhgar, B; Brewster, B (eds.), Combatting cybercrime and cyberterrorism, Springer International Publishing, 2016, pp. 175-192; Neil C. R., *The attribution of cyber warfare*, in: Green, J.A., Cyber warfare. A multidisciplinary analysis, Routledge, 2015, pp. 61-72; Guitton, C., *Inside the enemy's computer: identifying cyber attackers*, Oxford University Press, 2017, 320p; Tsagourias, N., *Cyber attacks, self-defence and the problem of attribution*, Journal of Conflict and Security Law, Vol. 17, No. 2, 2012, pp. 229-244; Kavaliauskas, A., *Can the concept of due diligence contribute to solving the problem of attribution with respect to cyber-attacks conducted by non-State actor which are used as proxies by States?*, Law Review, Vol. 26, No. 2, 2023, pp. 4-30; Eichensehr, K.E., *Decentralized cyberattack attribution*, American Journal of International Law, Vol. 113, 2019, pp. 213-217; Finlay, L.; Payne, C., *The attribution problem and cyber armed attacks*, American Journal of International Law, Vol. 113, 2019, pp. 202-206 and Healey, J.: *Beyond Attribution: Seeking National Responsibility in the Cyber Attacks*, Atlantic Council Issue Brief, [http://www.atlanticcouncil.org/images/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF] Accessed 10 June 2024.

Union, its Member States, or even to third countries or international organizations. There is undoubtedly a detailed clarification of the definition of a cyberattack[17], the factors[18] qualifying it as an external threat[19], and moreover, various essential concepts are defined to preclude any semblance of arbitrariness. For instance, the terms "freezing of funds"[20] or "freezing of economic resources"[21] are explicitly defined. In this paragraph, it is appropriate to address the territorial scope of the measures, as they extend beyond the territory or airspace of the Union. These measures may apply to aircraft or vessels under the jurisdiction of a Member State. Additionally, they are intended to encompass any natural or legal person who is a national or registered or incorporated under the laws of a Member State, or who conducts commercial activities, either wholly or partially, within the Union.

Thirdly, the recipients of the measures are specified: natural and/or legal persons, entities, or bodies, whether accountable for the action or attempt, included in the relevant annex.[22] Furthermore, the application of the measures will encompass those natural and/or legal persons who have provided financial, technical, or material assistance, or who have otherwise been implicated, for instance, through planning, preparation, or facilitation of such attacks by commission or omission. Finally, it was noted that if any form of association with natural or legal persons engaged in malicious activity were identified, those entities would be subject to the provisions of the established framework.

---

17 "[…] cyber-attacks are actions involving any of the following: a) access to information systems; b) information system interference; c) data interference; or d) data interception, where such actions are not duly authorized by the owner or by another right holder of the system or data or part of it, or are not permitted under the law of the Union or of the Member State concerned"

18 "[…]The factors determining whether a cyber-attack has a significant effect as referred to in Article 1(1) include any of the following: a) the scope, scale, impact or severity of disruption caused, including to economic and societal activities, essential services, critical State functions, public order or public safety; b) the number of natural or legal persons, entities or bodies affected; c) the number of Member States concerned; d) the amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property; e) the economic benefit gained by the perpetrator, for himself or for others; f) the amount or nature of data stolen or the scale of data breaches; or g) the nature of commercially sensitive data accessed"

19 "[…] Cyber-attacks constituting an external threat include those which: a) originate, or are carried out, from outside the Union; b) use infrastructure outside the Union; c) are carried out by any natural or legal person, entity or body established or operating outside the Union; or d) are carried out with the support, at the direction or under the control of any natural or legal person, entity or body operating outside the Union".

20 "[…] 'economic resources' means assets of every kind, whether tangible or intangible, movable or immovable, which are not funds, but may be used to obtain funds, goods or services"

21 "[…] freezing of economic resources' means preventing the use of economic resources to obtain funds, goods or services in any way, including, but not limited to, by selling, hiring or mortgaging them"

22 Vid. Case T-125/22 RT France v Council [2022] ECLI:EU:T:2022:483, para. 102.

Fourthly, the regulatory framework details the restrictive measures, comprising both the prohibition of entry or transit within Member States and the freezing of all funds and economic resources. However, nuanced exemption criteria were devised. For instance, nationals of Member States subject to these measures may have restrictions lifted regarding entry or transit. Additionally, compliance with consular/diplomatic law regarding privileges and immunities could lead to exemptions, particularly if a Member State hosts an international organization or an UN-sponsored conference attended by individuals subject to restrictions. Moreover, humanitarian justifications or legal proceedings may warrant the lifting of sanctions. Regarding exemptions for the freezing of funds and economic resources, a comprehensive range of exclusionary circumstances is contemplated. Verification may prompt the authorization of funds release to meet basic needs or cover reasonable professional fees and expenses for custody or maintenance services. Further exemptions encompass arbitral awards issued prior to inclusion, judicial or administrative resolutions issued by the Union or Member States, contracts concluded pre-inclusion, and allowance for third-party funds transfer into immobilized accounts, provided they are also retained. Lastly, provisions are established to absolve individuals or entities executing fund immobilization from liability if done in accordance with European regulations and in good faith.

In the fifth and final instance, the collaboration among the diverse implicated institutions - the Council, the Commission, and the Member States - at every phase of the sanctioning process is addressed. Communication coupled with coordination stands as a foundational pillar of the collective system. Consequently, they will exchange all pertinent information related to the execution and potential breaches of the provisions established both in the Regulation and the Decision. Accordingly, when a proposal for inclusion on the list is made by a Member State, the High Representative, or the Council, and it is deemed appropriate, the latter will communicate the decision, affording the opportunity to present relevant observations. Undoubtedly, in cases where observations are put forward or significant new evidence is presented, the Council will proceed with its examination. Hence, the list will undergo periodic review, at minimum every twelve months. The list will delineate the grounds for inclusion, as well as furnish the requisite details to identify the natural or legal persons, entities, or organisms concerned. Concerning natural persons, this information may encompass their full name, aliases, date and place of birth, nationality, passport or identity document number, gender, known postal address, and occupation or profession. As for legal persons, entities, or bodies, the list may encompass their full name, date and place of registration, registration number, and registered office address. With regard to the Member States, aside from endorsing regulations on sanctions for breaches of the prescribed provisions, they

will undertake the requisite measures to ensure their implementation.[23] In turn, the Commission will handle personal data within the purview of its competencies.[24] In summary, the cooperative framework among the implicated institutions underscores the importance of communication and collaboration in ensuring the effective implementation of the established measures. The periodic review of the list, along with the provision of comprehensive information, serves to maintain transparency and accountability within the regulatory regime. Moreover, the delineation of responsibilities between the Council, the Commission, and the Member States contributes to the overall efficacy and legitimacy of the sanctioning process.

The initial inclusion of six individuals and three legal entities took place through the mandatory Decision and implementing Regulation in July 2020.[25] Subsequently, the number rose the eight individuals and four legal entities within a few months.[26] These listings have been subject to annual extensions as prescribed by the regulatory framework. However, toward the end of 2023, a new exemption was introduced to enhance coherence and consistency between the Union's regime of restrictive measures and those adopted by the United Nations Security Council.[27] This exemption aimed to ensure the timely provision of humanitarian assistance or support for other activities addressing basic human needs. Specifically, an exemption from asset freezing measures and restrictions on making funds and economic resources available to designated individuals, entities, or bodies was instituted. This exemption benefited entities established under UN Security Council Resolution 2664 (2022), organizations and bodies granted the humanitarian partnership certificate by the UE, and organizations and bodies certified or recognized by a Member State or specialized agency thereof. Moreover, it was agreed to introduce an exception mechanism, or modify the existing one, for organizations and entities engaged in humanitarian activities ineligible for the exemption. Finally, it

---

23 The penalties provided for shall be effective, proportionate and dissuasive.

24 The Commission will carry out the following tasks: on the one hand, it will add the contents of the annex to the electronic, consolidated list of persons, groups and entities subject to Union financial sanctions and to the interactive sanctions map, both publicly available. On the other hand, it will be charge of processing.

25 Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States [2020] OJ L246/12. Council implementing Regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States [2020] OJ L246/ 4.

26 Council Decision (CFSP) 2020/1537 of 22 October 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States [2020] OJ L I/351/5.

27 Resolution 2664 (2022) on humanitarian exemptions to asset freeze measures imposed by UN sanctions regimes, adopted by the Security Council at its 9214th meeting, on 9 December 2022.

was deemed necessary to introduce review clauses concerning these exemptions. These clauses would facilitate periodic assessments of the exemption mechanism's effectiveness and relevance, ensuring alignment with evolving humanitarian needs and international security considerations. Therefore, this development signifies a proactive approach by the Union to harmonize its sanctions framework with global humanitarian imperatives, reflecting a commitment to balancing security objectives with humanitarian principles.[28]

3. THE EUROPEAN CHARTER OF FUNDAMENTAL RIGHTS: A SAFEGUARD AGAINST SANCTIONS FOR MALICIOUS CYBER ACTIVITIES?

In examining the issue at hand, it becomes evident that safeguarding fundamental rights is paramount in mitigating the adverse effects of sanctions levied against both individuals and legal entities in the realm of cyber activities. Of particular importance are the rights to good administration (as enshrined in article 41 of the ECFR) and to a fair trial (as articulated in article 47 ECFR).[29] Yet, equal attention must be given to the right to personal data protection (articulated in article 8 ECFR), especially concerning the assignment of malicious actions, the potential undue restriction on property rights (as stipulated in article 17 ECFR), and the adherence to the principle of proportionality (outlined in article 52 ECFR). Consequently, it becomes imperative to scrutinize the rationale put forth by the European Court of Justice (ECJ) regarding the criteria for including individuals or legal entities in sanction lists. This scrutiny not only ensures compliance with fundamental rights but also serves to uphold the integrity of the judicial process within the Union.[30] By carefully examining these legal principles and their application in the context of cyber-related sanctions, policymakers and legal practitioners can better navigate the complex landscape of cyber governance while upholding the values and principles outlined in the ECFR. Such an approach not only fosters a

---

[28] Council Decision (CFSP) 2023/2686 of 27 November 2023 amending certain Council Decisions concerning restrictive measures in order to insert provisions on humanitarian exceptions [2023] OJ L2023/2686. Council Regulation (EU) 2023/2694 of 27 November 2023amending certain Council Regulations concerning restrictive measures in order to insert provisions on humanitarian exceptions [2023] OJ L2023/2694.

[29] Bannelier, K., *Le standard de due diligence et la cyber-sécurité*, in: Société française pour le droit international, Le standard de due diligence et la responsabilité international, Journée d'études franco-italienne du Mans, Ed. A. Pedone, Paris, 2018, pp. 67-91.

[30] Cremona, M., *Effective Judicial Review Is of the Essence of the Rule of Law: Challenging Common Foreign and Security Policy Measures Before the Court of Justice*, 2 European Papers (2017), p. 671–697.

more just and equitable system but also strengthens the rule of law and promotes trust and confidence in European institutions.[31]

Whilst American judges has opted to apply lenient standards when deciding upon the imposition of restrictive measures, the ECJ has espoused the principle of comprehensive and rigorous judicial oversight to safeguard fundamental rights.[32] Consequently, the Council has encountered considerable setbacks in cases concerning sanctions.[33] A prime illustration of this **rigorous judicial scrutiny** within the EU framework is exemplified by the Kadi saga, a series of cases emblematic of the exhaustive judicial control exerted by the ECJ in matters involving the curtailment of individual rights.[34] Hence, the Court of Justice asserted in Kadi I that "the Community judicature [...] must ensure the full review of the lawfulness of all Union acts in the light of the fundamental rights forming an integral part of the European Union legal order" (par. 326).[35] Regarding **the right to defence**, Kadi II concluded that it "includes the right to be heard and the right to have access to the file, subject to legitimate interests in maintaining confidentiality" (par. 99).[36] In accordance with the requirements for considering a fair and due process, the judgment determined that it "requires that the person concerned must be able to ascertain the reasons upon which the decision taken in relation to him is based, either

---

31 Lazzerini, N., *Fundamental rights as constraints on the power of the European Union to impose sanctions*, in: Montaldo, S.; Costamagna, F.; Miglio, A., EU law enforcement. The evolution of sanctioning powers, Routledge, London, 2021, pp. 93-114.

32 Vid., Case C-562/13 *Centre public d'action sociale d'Ottignies-Louvain-La Neuve v Moussa Abdiva* [2014] ECLI:EU:C:2015:650, para. 45 and Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650, para. 95. See also Cantwell, D., *A tale of two Kadis: Kadi II, Kadi v. Geithner and US counterterrorism finance efforts*, The Columbia Journal of Transnational Law, Vol. 53, No. 3, 2015, pp. 653-700. Bogdanova, I.; Vásquez Callo-Müller, M., *Unilateral cyber sanctions: between questioned legality and normative value*, Vanderbilt Journal of Transnational Law, Vol. 54, No. 4, 2021, pp. 911-954.

33 Miadzvetskaya, Y., *Cyber sanctions: towards a European Union cyber intelligence service?*, College of Europe Policy Brief, No. 1, February 2021, [https://www.coleurope.eu/sites/default/files/research-paper/miadzvetskaya_cepob_1-2021_final_0.pdf], Accessed 10 April 2024; Simon, D., Rigaux, A., *Le jugement des pourvois dans les affaires "Kadi" et "Al Barakaat": "smart sanctions" pour le Tribunal de première instance?*, Europe 2008, Vol. 18, pp. 5-11.

34 Fabbrini, F.; Larik, J., *Global counter-terrorism sanctions and European due process rules: the dialogue between the CJEU and the ECtHR*, in Avbelj, M.; Fontanelli, F.; Martinico, G. (eds.), Kadi on trial: a multifaceted analysis of the Kadi judgment, Routledge, Abingdon: 2014, pp. 137- 156. Harpaz, G., *Judicial review by the European Court of Justice of UN "smart sanctions" against terror in the Kadi dispute*, European Foreign Affairs Review, Vol. 14, No. 1, 2009, pp. 65-88; Chachko, E., *Foreign Affairs in court: lessons from CJEU targeted sanctions jurisprudence*, Yale Journal of International law, Vol. 44, No. 1, 2018, pp. 1-51.

35 Join Cases C-402/05 & C-415/05 P *Yassin Abdullah Kadi & Al Barakaat International Foundation v. Council of the European Union,* [2008] ECR I-06351.

36 Join Cases C-584/10 P, C-593/10 P & C-595/10 P *European Commission and Others v Yassin Abdullah Kadi*, [2013] ECR – general.

by reading the decision itself or by requesting and obtaining disclosure of those reasons, without prejudice to the power of the court having jurisdiction to require the authority concerned to disclose that information, so as to make it possible for him to defend his rights in the best possible conditions and to decide, with full knowledge of the relevant facts, whether there is any point in his applying to the court having jurisdiction, and in order to put the latter fully in a position to review the lawfulness of the decision in question" (par. 100).[37]

Therefore, the decision to subject an individual or entity to specific restrictive measures requires clear criteria tailored to each specific case to determine which individuals and entities may be included in the list, which must also apply to the effects of their removal from the list.[38] Furthermore, the Council is bound by the obligation of reasoning established in article 296 of the TFEU, which implies that the reasoning identifies "not only the legal basis of that measure but also the individual, specific and concrete reasons why the competent authorities consider that the person concerned must be subject to restrictive measures" (par. 70).[39] The obligation of reasoning entails a robust argumentation which, however, could become vague and confusing considering the terms of the framework. Miadzvetskaya emphasizes that the flexibility inherent in the thematic sanctions system entails that concepts such as "significant effect" or "external threat" are not adequately defined.[40] Indeed, the Council set forth elements to assess whether an attack could be considered significant based on the scope, scale, impact, or severity of disruption caused and the number of "victims". However, as the author argues, ambiguity increases the risk of arbitrariness in decision-making and, consequently, increases the likelihood of being subject to judicial review.[41]

---

37 *Ibid*.

38 Vid., Case C-348/12 P *Council of the European Union v Manufacturing Support & Procurement Kala Naft Co., Tehran* [2013] ECLI:EU:C:2013:776, par. 73: "[…] Furthermore, the effectiveness of the judicial review guaranteed by Article 47 of the Charter also requires that the Courts of the European Union are to ensure that the decision, which affects the person or entity concerned individually, is taken on a sufficiently solid factual basis. That entails a verification of the allegations factored in the summary of reasons underpinning that decision, with the consequence that judicial review cannot be restricted to an assessment of the cogency in the abstract of the reasons relied on, but must concern whether those reasons, or, at the very least, one of those reasons, deemed sufficient in itself to support that decision, is substantiated".

39 Join Cases T-533/15 & T-264/16 *Il-Su Kim & Korea National Insurance Corporation v Council of the European Union & European Commission*, [2018] ECR-general.

40 Miadzvetskaya, Y., *op. cit.,* note 33, p. 3.

41 *Ibid.*

Much more has been decided regarding the right to defence and to be heard, for instance, in the RT France v Council case[42], the Court asserted that, although both rights are enshrined in the CFR as well as in jurisprudence, they are also subject to limitations or exceptions within the context of restrictive measures adopted under the CFSP.[43] On the one hand, it underlined that the existence of a violation of the right to defence must be assessed based on the specific circumstances of each case, particularly considering the nature of the act in question, the context in which it was adopted, and the legal norms governing the relevant matter.[44] On the other hand, with regard to the right to be heard, jurisprudence indicates that the Council is not obliged to inform the affected person or entity in advance of the reasons for their inclusion, as this would undermine the effectiveness of the measure. Consequently, the Court held that "such a derogation from the fundamental right to be heard during a procedure preceding the adoption of restrictive measures is justified by the need to ensure that the freezing measures are effective and, in short, by overriding considerations to do with safety or the conduct of the international relations of the Union and of its Member States" (par. 81).[45] In other words, the Court noted that the context made it difficult to adjust the restrictive measures due to the rapid deterioration of the situation and the severity of the violations committed. Indeed, the measures were adopted immediately after the onset of the military aggression, which was expected to be of short duration, thereby justifying the limitation (par. 87). [46] Therefore, the Court found that, given the "exceptionally urgent context" in which the contested acts were adopted, the right to be heard was not violated (par. 92).

With regard to the principle of good administration, according to established jurisprudence[47], the Council is obligated to thoroughly and impartially examine

---

42 Case T-125/22 *RT France v Council* [2022] ECLI:EU:T:2022:483.

43 *Ibid*., par. 77 "(see, to that effect, judgment of 21 December 2011, *France* v *People's Mojahedin Organization of Iran*, C27/09 P, EU:C:2011:853, paragraph 67 and the case-law cited) and in other spheres (see, to that effect, judgments of 15 June 2006, *Dokter and Others*, C28/05, EU:C:2006:408, paragraphs 75 and 76, and of 10 September 2013, *G. and R.*, C383/13 PPU, EU:C:2013:533, paragraph 33).

44 *Ibid*., par. 78.

45 See to that effect, Case C27/09 P *France* v *People's Mojahedin Organization of Iran*, EU:C:2011:853, par. 67.

46 Case T-125/22, op. cit., note 42, par. 87. "Thus, in the context of the European Union's overall strategy of responding in a rapid, united, graduated and coordinated manner, the requirements of urgency and effectiveness of all the restrictive measures adopted justified the limitation, on the basis of Article 52(1) of the Charter (see paragraph 77 above), of the application of Article 41(2)(a) of the Charter, inasmuch as they responded effectively to objectives of general interest recognised by the European Union, such as protecting the Union's public order and security, as stated in recital 8 of the contested acts".

47 Case T-545/13 *Fahed Mohamed Sakher al Matri v Council of the European Union* [2016] ECLI:EU:T:2016:376.

all relevant circumstances of the case when adopting restrictive measures. In the Kaddour case[48], it was held that the mere inclusion of the applicant's name on the lists could not, by itself, be sufficient to question the Council's impartiality. Furthermore, the Court clarified that the prolonged presence of his name on the lists could not, in itself, be considered indicative of partial or inequitable treatment, nor of unreasonable delay in the handling of his case (par. 55).

Another important aspect lies in the evidence, as elucidated in Kadi II, it must be "substantiated and that it constitutes in itself sufficient basis to support that decision" (par. 130).[49] Hence, when transposed into our cyber realm, this obligation becomes intricate due to the inherent challenges in gathering evidence, particularly concerning anonymity. Moreover, another increasingly significant challenge emerges: attribution, or establishing the link between malicious activities and their perpetrators. In this context, the right to personal data protection assumes crucial importance, as evidence collection may necessitate confidentiality, potentially leaving individuals vulnerable.[50] It is notable that the EU has ruled that imposing restrictive measures does not imply attributing international responsibility to third States.[51] Therefore, the Union is empowered to target the perpetrators of attacks (be they individuals or non-state entities) based on technical attribution, reserving the invocation of international responsibility for States. However, Brussels' stance, while politically motivated, adds complexity in pinpointing the true culprits behind cyberattacks. The evidentiary challenges might be addressed by adhering to the criterion established in the Anbouba case[52], where it was specified that the Council had met the burden of proof by presenting to the Union judge a set of sufficiently concrete, precise, and consistent evidence. This evidence allowed for the establishment of a sufficient link between the individual subject to a restrictive measure (par. 53).[53]

The **restriction of property** could likewise be subject to review by the Court. However, in Kadi I, it was prescribed that such a measure was not intended nor had the effect of subjecting individuals listed in the consolidated list to inhuman or degrading treatment. In the Rosneft case[54], the Court underscored the extensive

---

48 Case T-461/15 *Khaled Kaddour v Council of the European Union* [2018] ECLI:EU:T:2018:316.

49 Join Cases C-584/10 P, C-593/10 P & C-595/10 P…, *op. cit.,* note 36.

50 Case C-280/12 P *Council v Fulmen and Mahmoudian* [2013] ECLI:EU:C:2013:775, par. 59 and 60.

51 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, Vol. 24, 2023, pp. 522-536.

52 Case C-630/13 P *Issam Anbouba v Council of the European Union* [2015] ECLI:EU:C:2015:247.

53 Vid. Case C-193/15 P *Tarif Akhras v Council of the European Union* [2016] ECLI:EU:C:2016:219.

54 Case C-72/15 PJSC, op. cit., note 15. For a comment on Rosneft case, see, Poli, S., *The Common Foreign Security Policy after Rosneft: Still imperfect but gradually subject to the rule of law*, Common Market

discretionary authority vested in the legislator when making political, economic, and social decisions, which often require intricate assessments (par. 146 and 147). The Court concluded that the fundamental rights at issue—freedom of enterprise and property rights—are not absolute prerogatives. Their exercise may be legitimately restricted by the Union to achieve objectives of general interest (par. 148).[55]

Concerning judicial control over the observance of the principle of proportionality, the Court in the Hawswani case reiterated that, in accordance with jurisprudence, this principle "requires that measures implemented through provisions of EU law should be appropriate for attaining the legitimate objectives pursued by the legislation concerned and do not go beyond what is necessary to achieve them" (par. 99).[56] Furthermore, the Court clarified that it had recognized the European legislator's "broad discretion in areas involving political, economic, and social choices, where complex assessments are required" (par. 100).[57] Consequently, when the time comes, the Council would need to demonstrate that the adoption of restrictive measures is appropriate, as alternative and less coercive measures would not effectively achieve the intended purpose.[58]

Finally, it is relevant to examine the possibility of compensation for damages allegedly suffered as a consequence of the established restrictive measures. In light of the necessary coherence of the judicial protection system established by Union law, the Court is also competent to rule on the damages allegedly suffered due to restrictive measures adopted in CFSP decisions. The primary reason is that the public designation of individuals subject to restrictive measures brings opprobrium and mistrust, which can cause damages and justify the filing of a compensation claim to seek redress. The Court's approach can be observed in three significant cases: Abdulrahim[59], Safa Nicu

---

Law Review, Vol. 57, 2017, pp. 1799-1834.

55 *Ibid*., par. 148 "[…] Second, the fundamental rights relied on by Rosneft, namely the freedom to conduct a business and the right to property, are not absolute, and their exercise may be subject to restrictions justified by objectives of public interest pursued by the European Union, provided that such restrictions in fact correspond to objectives of general interest and do not constitute, in relation to the aim pursued, a disproportionate and intolerable interference, impairing the very essence of the rights guaranteed (see, to that effect, judgments of 14 May 1974, Nold v Commission, 4/73, EU:C:1974:51, paragraph 14; of 30 July 1996, Bosphorus, C84/95, EU:C:1996:312, paragraph 21, and of 16 November 2011, Bank Melli Iran v Council, C548/09 P, EU:C:2011:735, paragraphs 113 and 114)".

56 Case C241/19 P *George Haswani v Council of the European Union & European Commission* [2020] not yet published ECR.

57 *Ibid.*

58 Case C-348/12 *Bank Melli Iran v Council T-390/08* [2009] ECLI:EU:C:2013:77.

59 Case C-239/12 P *Abdulbasit Abdulrahim v Council of the European Union & European Commission* [2013] ECLI:EU:C:2013:331.

Sepahan[60], and Bank Refah Kargaran.[61] The Grand Chamber ruling in Abdulrahim constituted the first, albeit timid and indirect, signal of openness towards recognizing the applicant's right to some form of reparation, at least for non-material damages suffered as a result of the imposition of restrictive measures. [62] In this case, however, such reparation consisted solely of the rehabilitation of the applicant's reputation resulting from the annulment of the act adopted against him, and not from pecuniary compensation.[63] However, it was not until the Safa Nicu Sepahan case that the Court recognized, for the first time, monetary compensation for the damage suffered as a result of being listed under restrictive measures. Thus, not only would the annulment of the restrictive measures constitute a form of reparation for non-material damage, but the individual or entity could also seek pecuniary compensation. To determine the amount of compensation, particular consideration was given to the gravity of the observed violation, its duration, the behaviour of the Council, and the effects of the implication on third parties (par. 52). It is notable that, despite acknowledging the damage, the Court limited the amount to 50,000 euros. This apparent novelty faced an impasse in the Bank Refah Kargaran case. Although nothing prevents the applicant from invoking, in a compensation claim like the one leading to the contested judgment, an illegality consisting of the violation of the right to effective judicial protection, the failure to fulfil the obligation to state reasons could not, by itself, generate the Union's liability (par. 62 and 63). Indeed, the Court continued by clarifying that the obligation to state reasons, established in Article 296 TFEU, constitutes a substantive formal requirement that must be distinguished from the question of the adequacy of the reasoning, as this pertains to the legality of the contested act on the merits. In effect, the reasoning of a decision involves formally expressing the grounds on which that decision is based. If these grounds are unsustainable or flawed, they vitiate the legality of the decision on the merits, but not its reasoning (par. 64).

4. CONCLUSION

The thematic approach of cyber sanctions presents a unique flexibility compared to country-specific measures. By updating existing sanction lists instead of creating new legal frameworks, it streamlines the process and avoids lengthy, veto-prone procedures often seen with specific country designations. This adaptability resonates well with the dynamic nature of cyberspace, where States frequently col-

---

60 Case C-45/15 P *Safa Nicu Sepahan Co. v Council of the European Union* [2017] ECLI:EU:C:2017:402.

61 Case C-134/19 P *Bank Refah Kargaran v Council of the European Union* [2020] ECLI:EU:C:2020:793.

62 Vid. Case T-328/14 *Jannatian v Council* [2016] EU:T:2016:86, par. 62–63.

63 Messina, M., *The European Union's non contractual liability following country and counterterrorism sanctions: Is there anything to learn from the Safa Nicu Sepahan case?*, Maastricht Journal of European and Comparative Law, Vol. 25, No. 5, 2018, p. 643.

laborate with non-state actors to further their strategic goals[64]. However, amidst this flexibility lies a potential challenge: the legislative framework's ambiguity. Such ambiguity could lead to judicial review and possibly annulment, jeopardizing the legitimacy and effectiveness of the sanctions. This raises questions about the stagnant sanction list, unchanged since 2020, and whether it reflects a broader model fatigue.

The infrequent updates to the list raise concerns about the framework's ability to address evolving cyber threats adequately. With technology advancing rapidly and cyber threats constantly evolving, a static list may fall short in effectively combating emerging challenges. Moreover, the lack of updates may signal a failure to adapt to shifting geopolitical dynamics and emerging cyber threats. Additionally, the inherent ambiguity in the legislative framework poses implementation and enforcement challenges. Unclear criteria for inclusion on the sanction list and designation processes may lead to inconsistencies and errors, undermining the sanctions' legitimacy and effectiveness in deterring malicious cyber activities.

The effectiveness of judicial review guaranteed by Article 47 of the Charter of Fundamental Rights of the European Union requires that, when examining the legality of the reasons underlying the decision to include a person's name on the list of those subject to restrictive measures, the Union judge must ensure that such a decision, which constitutes an individual act for that person, is based on sufficiently solid factual grounds. This involves verifying the facts alleged in the statement of reasons underpinning the contested acts to determine whether such reasons, or at least one of them deemed sufficient on its own, are well-founded.

In assessing the importance of the interests at stake, which forms part of the proportionality review of the discussed restrictive measures, the context in which these measures are integrated must be taken into account. This assessment should be carried out by examining the evidence, not in isolation, but within the context in which it is situated. Given the difficulty for the Council to provide evidence due to complex situations, it meets its burden of proof if it presents to the Union judge a set of sufficiently concrete, precise, and consistent indications that establish a sufficient link between the person subject to a restrictive measure and the situation addressed by the measure. Moreover, provided that the evidence has been obtained regularly and that the general principles of law and procedural rules applicable to the burden and presentation of proof have been observed, it is for the General Court alone to assess the value to be attributed to the elements presented. Furthermore, Article 47 of the Charter of Fundamental Rights of the European

[64] Miadzvetskaya, Y., *op. cit.,* note 31, p. 4.

Union, which reaffirms the principle of effective judicial protection, stipulates in its first paragraph that everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal, under the conditions set out in that article. The very existence of effective judicial review to ensure compliance with Union law is inherent to the existence of the rule of law.

REFERENCES

BOOKS AND ARTICLES

1. Bannelier, K., *Le standard de due diligence et la cyber-sécurité*, in: Société française pour le droit international, Le standard de due diligence et la responsabilité international, Journée d'études franco-italienne du Mans, Ed. A. Pedone, Paris, 2018, pp. 67-91
2. Bendiek, A.; Schulze, M., *Attribution: a major challenge for EU cyber sanctions*, German Institute for International and Security Affairs, SWP Research Paper No.11, December 2021, Berlin
3. Bogdanova, I.; Vásquez Callo-Müller, M., *Unilateral cyber sanctions: between questioned legality and normative value*, Vanderbilt Journal of Transnational Law, Vol. 54, No. 4, 2021, pp. 911-954
4. Cantwell, D., *A tale of two Kadis: Kadi II, Kadi v. Geithner and US counterterrorism finance efforts*, The Columbia Journal of Transnational Law, Vol. 53, No. 3, 2015, pp. 653-700
5. Chachko, E., *Foreign Affairs in court: lessons from CJEU targeted sanctions jurisprudence*, Yale Journal of International law, Vol. 44, No. 1, 2018, pp. 1-51
6. Cremona, M., *Effective Judicial Review Is of the Essence of the Rule of Law: Challenging Common Foreign and Security Policy Measures Before the Court of Justice*, 2 European Papers (2017), p. 671–697
7. Delerue, F., *Cyberoperations and international law*, Cambridge University Press, 2020, 513p
8. Eichensehr, K.E., *Decentralized cyberattack attribution*, American Journal of International Law, Vol. 113, 2019, pp. 213-217
9. Fabbrini, F.; Larik, J., *Global counter-terrorism sanctions and European due process rules: the dialogue between the CJEU and the ECtHR*, in Avbelj, M.; Fontanelli, F.; Martinico, G. (eds.), Kadi on trial: a multifaceted analysis of the Kadi judgment, Routledge, Abingdon: 2014, pp. 137- 156
10. Finlay, L.; Payne, C., *The attribution problem and cyber armed attacks*, American Journal of International Law, Vol. 113, 2019, pp. 202-206
11. Guitton, C., *Inside the enemy's computer: identifying cyber attackers*, Oxford University Press, 2017, 320p
12. Harpaz, G., *Judicial review by the European Court of Justice of UN "smart sanctions" against terror in the Kadi dispute*, European Foreign Affairs Review, Vol. 14, No. 1, 2009, pp. 65-88
13. Hörbelt, C., *A comparative study: where and why does the EU impose sanctions*, Revista Unisci/ Unisci Journal, No. 43, January 2017, pp. 53-71

14. Kasper, A.; Osula, A.M.; Molnár, A, *EU cybersecurity and cyber diplomacy,* Revista d'internet, dret i política, Dossier "Europe facing the digital challenge: obstacles and solutions", No. 34, December, 2012, pp. 1-15
15. Kavaliauskas, A., *Can the concept of due diligence contribute to solving the problem of attribution with respect to cyber-attacks conducted by non-State actor which are used as proxies by States?*, Law Review, Vol. 26, No. 2, 2023, pp. 4-30
16. Kijeweski, P.; Jaroszewski, P.; Urbanowicz, J.A.; Armin, J., *The never-ending game of cyber-attack attribution*: *Exploring the threats, defenses and research gaps* in: Akhgar, B; Brewster, B (eds.), Combatting cybercrime and cyberterrorism, Springer International Publishing, 2016, pp. 175-192
17. Lazzerini, N., *Fundamental rights as constraints on the power of the European Union to impose sanctions*, in: Montaldo, S.; Costamagna, F.; Miglio, A., EU law enforcement. The evolution of sanctioning powers, Routledge, London, 2021, pp. 93-114
18. Messina, M., *The European Union's non contractual liability following country and counterterrorism sanctions: Is there anything to learn from the Safa Nicu Sepahan case?*, Maastricht Journal of European and Comparative Law, Vol. 25, No. 5, 2018, pp. 632-648
19. Miadzvetskaya, Y.; Wessel, Ramses A., *The externalization of the EU's cybersecurity regime: the cyber diplomacy toolbox*, European Papers, Vol. 7, No. 1, 2022, pp. 413-438
20. Neil C. R., *The attribution of cyber warfare*, in: Green, J.A., Cyber warfare. A multidisciplinary analysis, Routledge, 2015, pp. 61-72
21. Pawlak, P., *The EU's Role on Shaping the Cyber Regime Complex*, European Foreign Affairs Review Vol. 24, No. 2, 2019, pp. 167-186
22. 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, Vol. 24, 2023, pp. 522-536
23. Simon, D., Rigaux, A., *Le jugement des pourvois dans les affaires "Kadi" et "Al Barakaat": "smart sanctions" pour le Tribunal de première instance?*, Europe 2008, Vol. 18, Novembre, pp. 5-11
24. Tsagourias, N., *Cyber attacks, self-defence and the problem of attribution*, Journal of Conflict and Security Law, Vol. 17, No. 2, 2012, pp. 229-244

WEBSITE REFERENCES

1. [http://www.ieee.es/Galerias/fichero/docs_opinion/2020/DIEEEO143_2020MARROB_ciberUE.pdf], Accessed 10 April 2024
2. Arteaga, F., *Sanciones contra los ciberataques: la UE enseña las uñas*, Real Instituto Elcano, Comentario Elcano 19/2019, 11.06.2019, [https://media.realinstitutoelcano.org/wp-content/uploads/2021/11/comentario-arteaga-sanciones-contra-los-ciberataques-la-ue-ensena-las-unas.pdf], Accessed 10 April 2024
3. Borrell, J., *Cyber sanctions: time to act*, 30.07.2020, [https://www.eeas.europa.eu/eeas/cyber-sanctions-time-act_en], Accessed 10 April 2024

4. Healey, J.: *Beyond Attribution: Seeking National Responsibility in the Cyber Attacks*, Atlantic Council Issue Brief, [http://www.atlanticcouncil.org/images/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF], Accessed 10 June 2024
5. Miadzvetskaya, Y., *Cyber sanctions: towards a European Union cyber intelligence service?*, College of Europe Policy Brief, No. 1, February 2021, [https://www.coleurope.eu/sites/default/files/research-paper/miadzvetskaya_cepob_1-2021_final_0.pdf], Accessed 10 April 2024
6. Moret, E.; Pawlak, P., *The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?*, European Union Institute for Security Studies (EUISS), Brief Issue No. 24, 2017, [https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/EUISS-Brief_24_Cyber_sanctions.pdf], Accessed 10 April 2024
7. Robles Carrillo, M., *Sanciones contra ciberataques: la acción de Unión Europea*, Documento de Opinión IEEE 143/2020