La unión europea como actor internacional en materia de ciberseguridad

The european union as an international actor in cybersecurity

Juan Jorge Piernas López
Senior Lecturer ('Profesor Titular')
Public International Law and International Relations
University of Murcia
Jean Monnet Chair

Recibido: 15.06.2022 / Aceptado: 11.07.2022
DOI: 10.20318/cdt.2022.7202

Abstract: This article analyzes the role of the European Union as an international actor in Cybersecurity. For these purposes, the article assesses, first, the evolution of the external dimension of the European Union Cybersecurity policy, with particularly reference to the 2013 Cybersecurity strategy. Second, the paper studies the emergence and development of the EU Cyber diplomacy. Third, the article examines the novelties related to the role of the EU as an international actor introduced by the 2020 Cybersecurity strategy and subsequent documents such as the 2022 Strategic Compass and Cyber posture. Finally, a number of conclusions are drawned in the last section.
Keywords: Cybersecurity, external dimension, EU as an international actor, evolution.

Resumen: Este artículo analiza el papel de la Unión Europea como actor internacional en materia de ciberseguridad. Para ello, el artículo evalúa, en primer lugar, la evolución de la dimensión exterior de la política de Ciberseguridad de la Unión Europea, con especial referencia a la estrategia de Ciberseguridad de 2013. En segundo lugar, el artículo estudia el surgimiento y desarrollo de la Ciberdiplomacia de la UE. En tercer lugar, el artículo examina las novedades relacionadas con el papel de la UE como actor internacional introducidas por la estrategia de Ciberseguridad de 2020 y documentos posteriores como la Brújula Estratégica y la postura cibernética de la Unión, aprobados en 2022. Finalmente, en la última sección se extraen una serie de conclusiones.
Palabras claves: Ciberseguridad, dimensión exterior, la UE como actor internacional, evolución.

I. Introduction

1. Cybersecurity law and policy are concerned with matters that, by their very nature, transcend the EU borders. Indeed, as it has been noted, the development of EU Cybersecurity policy area was triggered by global security threats,[1] and the Union recognized the need for an international EU Cyber security policy almost ten years ago, in the 2013 Cybersecurity Strategy.

[1] This study is the result of the work carried out by the author in the framework of the research project "The search for an international regulation of cybernetic activities: an unavoidable necessity? (CYBINREG)", Aid for R&D&I Projects within

2. Cybersecurity, as part of "security", is one of the areas to which the Union is committed to contribute in its relations with the rest of the world, in accordance with Article 3(5) TEU,[2] and which the Union shall defend in international relations, as set out in Article 21(2) TEU.[3] However, as recently held, "the Treaties do not provide for concrete legal bases to adopt measures to prevent or counter external cyber threats or attacks. This forced the Union to be creative and use existing legal bases (inter alia on restrictive measures or defence policy) and cooperation frameworks (such as PESCO)."[4]

3. In this context, this article is concerned with the analysis of the external dimension of the European Union Cybersecurity policy, including the emergence and development of the EU Cyber diplomacy. In this regard, as underlined by Odermatt, "it is in the external dimension of cybersecurity policy where the EU can potentially have a greater impact, by co-operating with states, international organisations and non-state bodies, and by influencing the development of norms at the international level".[5]

4. The article will thus examine the impact that the EU has had as an international actor in the field of cybersecurity,[6] notably by cooperating with international players and by influencing the development of international norms and standards. For these purposes, the article will examine relevant policy documents adopted in this area, including the 2013 and 2020 Cybersecurity strategies, the 2022 Strategic Compass and Cyber posture, as well as the legal framework related to the role of the EU as an international actor in cybersecurity, notably in relation to the adoption of restrictive measures in the event of a cyber-attack.

II. The external dimension of EU cybersecurity and the 2013 Cybersecurity strategy

5. Cybersecurity policy has evolved from a field of action initially linked to cybercrime under Article 83 TFEU, towards a policy closely related to the functioning of the internal market, as shown by the fact that the NIS Directive, the first cybersecurity legislative act in the strict sense, was adopted under Article 114 TFEU.[7] This trend has been confirmed by other measures, including the adoption of Regulation (EU) 2019/881 of the European Parliament and of the Council, the so-called "Cybersecurity Act", or the proposal of the NIS 2 Directive under the same legal basis.[8]

6. The adoption of measures under the ordinary legislative procedure reveals that Union action in this area has come to be considered as necessary, in accordance with the principle of subsidiarity, so-

the framework of the State Programmes for the generation of knowledge and scientific and technological strengthening of the R&D&I system oriented towards the challenges of Society (Ref PID 2020 112577 RB I 00) (Call 2020), whose Principal Investigator I is Professor María José Cervell Hortal and Principal Investigator II is Professor Juan Jorge Piernas López.

R.A. Wessel, "Towards EU cybersecurity law: Regulating a new policy field", in N. Tsagourias/ R. Buchan, (Eds.), *International Law and Cyberspace*, *Research Handbooks in International Law series*, Edward Elgar, 2016, pp. 403-425, at p. 404.

[2] Article 3(5) TEU provides that "In its relations with the wider world, the Union shall uphold and promote its values and interests and contribute to the protection of its citizens. It shall contribute to peace, security, the sustainable development of the Earth, solidarity and mutual respect among peoples, free and fair trade, eradication of poverty and the protection of human rights, in particular the rights of the child, as well as to the strict observance and the development of international law, including respect for the principles of the United Nations Charter ".

[3] According to Article 21(2) TEU "The Union shall define and pursue common policies and actions, and shall work for a high degree of cooperation in all fields of international relations, in order to: (a) safeguard its values, fundamental interests, security, independence and integrity […]".

[4] Y. Miadzvetskaya/ R.A. wessel, "The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox", European Papers, 2022, forthcoming, at page 25.

[5] J. Odermatt, "The European Union as a Cybersecurity Actor", in S. blockmans & p. koutrakos (eds), Research Handbook on EU Common Foreign and Security Policy, Cheltenham/Northhampton: Edward Elgar Publishing, 2018, pp. 354-373, at p. 369.

[6] See in this regard also A. Barrinha and H. Varrapiço "The EU's security actorness in cyber space: quo vadis?", in L Chappell, J Mawdsley, and P Petrov (eds.), *The EU, strategy and security policy: regional and strategic challenges*, Routledge, 2016, pp. 104-118.

[7] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union OJ L 194, 19.7.2016, p. 1–30.

[8] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM/2020/823 final.

mething that may *prima facie* contrast with the fact that national security, which is closely related to cybersecurity, remains the sole responsibility of the Member States, as unambiguously stipulates Article 4(2) of the Treaty on European Union, and recently underlined the 2019 EU Cyber Security Act.[9] Similarly, Article 72 TFEU reminds that measures in the area of freedom, security and justice, such as the measures to prevent and combat cybercrime, shall not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security.

7. In this context, the origin of the external dimension of cybersecurity is often traced back to February 2013, when the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy jointly presented the "EU Cybersecurity Strategy: Open, Secure and Safe Cyberspace"[10]. The Strategy underlined that governments across the world had started to consider cybersecurity as an increasingly important international issue,[11] and included the establishment of "a coherent international cyberspace policy for the European Union and promote core EU values" as one of the EU's five strategic priorities in this area.[12]

8. Notwithstanding, the 2008 Report on the Implementation of the European Security Strategy had already identified cyber security as one of the global challenges and key threats, noting that more work was required in this area, particularly to "enhance international co-operation."[13] In addition, the European Commission had underlined in 2009 the importance of "engaging the global community to develop a set of principles, reflecting European core values, for Internet resilience and stability, in the framework of our strategic dialogue and cooperation with third countries and international organisations".[14] The Commission also mentioned in the same communication a number of international initiatives such as NATO activities on common policy on cyber defence, the 2003 G8 principles for Protecting Critical Information Infrastructures, the UN General Assembly Resolution 58/199 Creation of a global culture of cybersecurity and the protection of critical information infrastructures, or the OECD Recommendation on the Protection of Critical Information Infrastructures.[15]

9. Similarly, also in the context of the protection of ICT in critical infrastructures, the European Commission stated in 2011 that "A purely European approach is not sufficient to address the challenges ahead. Although the objective of building a coherent and cooperative approach within the EU remains as important as ever, it needs to be embedded into a global coordination strategy reaching out to key partners, be they individual nations or relevant international organisations. "[16]

10. In any event, the 2013 EU Cybersecurity Strategy consolidated previous efforts and outlined the way forward. The Strategy also underlined that the principles, values and standards that the EU promotes offline must be applied online, and in particular that fundamental rights, democracy and the rule of law must be protected in cyberspace".[17]

---

[9] See in this regard R.A. wessel, 'European Law and Cyberspace', in N. tsagourias and R. buchan (Eds.), *International Law and Cyberspace*, Cheltenham/Northhampton: Edward Elgar Publishing, 2021, pp. 490-507, at pp. 491-492.

[10] JOIN/2013/01 final, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.

[11] Id., at 3.

[12] Id. at 5.

[13] Report on the Implementation of the European Security Strategy - Providing Security in a Changing World -, Brussels, 11 December 2008 S407/08, p. 5.

[14] "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (COM/2009/0149 final), p. 7. See also in this regard a. kasper and v. vernygora, "The EU's cybersecurity: a strategic narrative of a cyber power or a confusing policy for a local common market?", Cuadernos Europeos de Deusto, No. 65/2021, Bilbao, pp. 29-71, at p.50.

[15] Id., p. 3.

[16] Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security', COM/2011/0163 final, p. 4.

[17] JOIN(2013) 1 final, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "EU Cybersecurity Strategy: Open, Secure and Safe Cyberspace", paragraph 1.1.

11. The Strategy also highlighted that cybersecurity is multidimensional in nature, affecting both the Union's economic policies, in particular the internal market [and the digital single market], as well as the more intergovernmental policies, such as the common security and defence policy and, more generally, the Union's external action. Indeed, the dual authorship of the Strategy, namely the Commission and the High Representative for Foreign Affairs and Security Policy, already underlined the need to combine the internal and external dimensions of EU policies to effectively address cybersecurity challenges. On the other hand, any EU cybersecurity policy must also take into account the actions of the Member States, and coexist with measures taken at national level, given the absence of any explicit EU competence in the field of security, let alone cybersecurity, in the Treaties, and the fact that the Treaties underline that national security will remain, as mentioned before, the sole responsibility of each Member State.

12. In addition, as the Strategy remarked, cybersecurity policy should also involve the private sector and public-private partnerships. In this context, it is worth recalling that Article 21(3) TEU states, *in fine*, that the Union "The Union shall ensure consistency between the different areas of its external action and between these and its other policies. The Council and the Commission, assisted by the High Representative of the Union for Foreign Affairs and Security Policy, shall ensure that consistency and shall cooperate to that effect." This principle of coherence, as it has been noted, incorporates formal obligations that can be invoked before the Court of Justice, which could condemn its violation.[18]

13. Indeed, the Strategy provided a definition of cybersecurity in the following terms: "Cybersecurity commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein"[19].

14. The Strategy also defined the concept of cybercrime in broad terms,[20]which seemingly go beyond the notion of "computer-related crime" under Article 83 TFEU[21] to reflect, as it has been held, the conducts foreseen by the Budapest Cybercrime convention.[22] In this context, the Strategy recognised that "it is predominantly the task of Member States to deal with security challenges in cyberspace" and therefore limited itself to proposing concrete measures that could "enhance the EU's overall performance"[23]. Specifically, the Strategy identified five priorities in this area, namely:

— **Achieving cyber resilience**[24] , for which the Commission proposed, among other measures, the adoption of a Directive to promote a high common level of network and information se-

[18] C. Hillion, "A Powerless Court? The European Court of Justice and the EU Common Foreign and Security Policy", 2014, available at SSRN: https://ssrn.com/abstract=2388165. "Arguably, these two principles [coherence and loyal cooperation] located outside the specific TEU chapter on CFSP, and particularly the procedural obligations derived therefrom are in principle enforceable before the Court of Justice, irrespective of the fact that EU institutions are operating within the CFSP context".

[19] JOIN(2013) 1 final, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "EU Cybersecurity Strategy: Open, Secure and Safe Cyberspace", paragraph 1.1. Footnote 4.

[20] Id., footnote 5:"Cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware)."

[21] Article 83 TFEU empowers the European Parliament and the Council to establish, by means of directives adopted in accordance with the ordinary legislative procedure, minimum rules concerning the definition of criminal offences and sanctions in certain areas of crime which are, *inter alia,* of particular gravity and have a cross-border dimension resulting from their nature, in particular "terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime ".

[22] See in this regard R.A. wessel, 'European Law and Cyberspace', in N. tsagourias and R. buchan (Eds.), *International Law and Cyberspace*, cit, at p. 493.

[23] JOIN(2013) 1 final, cit., paragraph 2.

[24] On the concept of resilience in the European Union and its link to security see G. christou, *Cybersecurity in the European Union Resilience and Adaptability in Governance Policy*, Palgrave Macmillan, 2015, in particular pp. 11-34.

curity across the Union, which would be finally adopted in 2016[25], and that will be replaced by the NIS 2 Directive, currently under discussion.[26]

— **Drastically reducing cybercrime**, for which it called on Member States, among other measures, to ratify the abovementioned Council of Europe Convention on Cybercrime, done in Budapest on 23 November 2001, and to implement its measures as soon as possible. In this context, the fight against cybercrime, and in particular against cyber-attacks, is one of the EU priorities concerning serious and organised international crime and there is a clear trend towards focusing on the prevention of cyber-attacks in this area. To this extent, the EU priorities for the fight against serious and organised international crime between 2022 and 2025, as approved by the Council of the Union at its meeting of 12 May 2021, include the following priority: "to target the criminal offenders orchestrating cyber-attacks, particularly those offering specialised criminal services online". [27]

— **Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)**, including an EU Cyber Defence policy framework to protect networks within CSDP missions and operations, finally adopted by the Council in 2014[28]. The Cyber Defence policy framework was substantially revised in 2018, in a context of increased ambition in the Union's response to threats from cyberspace[29].

— **Develop the industrial and technological resources for cybersecurity by** requesting in particular the then ENISA, and currently European Union Agency for Cybersecurity (ENISA), to develop technical guidelines and recommendations for the adoption of NIS standards and best practices in the public and private sectors.

— **Establish a coherent international cyberspace policy for the European Union and promote core EU values**.

15. In relation to this priority for action, the most relevant for the purposes of this work, the EU Strategy recognised the global dimension of cybersecurity challenges and the need to integrate cyberspace issues into the EU's external relations and common foreign and security policy. It also expressed a commitment to work with international actors in this field. In particular the Strategy mentioned the Council of Europe, the Organization for Economic Co-operation and Development (OECD), the United Nations, the Organization for Security and Co-operation in Europe (OSCE), the North Atlantic Treaty Organization (NATO), the African Union, the Association of Southeast Asian Nations (ASEAN) and the Organization of American States (OAS), as well as national actors, such as the United States, with which the EU has had a working group on Cybersecurity and Cybercrime since 2010[30] .

16. In this respect, the Strategy referred to the reports of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, which conclude that international law, and the UN Charter in particular, are applicable to cyberspace[31]. Indeed, subsequent documents of the aforementioned Group of Experts have been even more

[25] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1-30.

[26] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM/2020/823 final.

[27] Council conclusions setting the EU's priorities for the fight against serious and organised crime for EMPACT 2022 - 2025, 8428/1/21 REV 1. The conclusions add the following in this context: "This priority should be implemented in one Operational Action Plan (1 OAP). Experiences gained from the implementation of the "cyber-attacks" OAP in the current EMPACT Cycle should be duly taken into consideration. "

[28] Council document No 15585/14 of 18.11.2014.

[29] EU Cyber Defence Policy Framework (2018 update), Brussels, 19 November 2018, 14413/18.

[30] JOIN(2013) 1 final, cit., p. 16. For the EU-US working group see, among others, the following link https://ec.europa.eu/commission/presscorner/detail/en/PRES_10_315.

[31] In particular reference is made to the 2013 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98). Regarding the application of international law to cyberspace and the responses that international law offers to states that are victims of cyber-attacks, see H. Moynihan, "The Application of International Law to State Cyberattacks Sovereignty and Non-intervention", *Research*

detailed: "In their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States. Existing obligations under international law are applicable to State use of ICTs. States must comply with their obligations under international law to respect and protect human rights and fundamental freedoms"[32].

17. In relation to the foregoing, the Strategy clearly stated that the Union did not see the need for new rules of international law in this area - a view that may have changed recently in relation to the proposal of the UN convention on cybercrime as will be discussed below- but rather to implement existing law and promote rules of conduct, a thesis that seems to have now taken hold[33]. In the Strategy's unequivocal terms: "The EU does not call for the creation of new international legal instruments for cyber issues"[34] .

III. The emergence and development of EU cyberdiplomacy

18. The 2013 Cybersecurity Strategy did not include a specific mention to cyber diplomacy. However, both the Strategy[35] and the EU Action Plan for Human Rights and Democracy[36], addressed issues that are related to the current notion of cyber diplomacy, for example the need to defend EU values both online and offline, including fundamental rights, and in particular freedom of expression, in cyberspace[37].

19. In any event, the lack of specific references to cyber diplomacy was addressed by the Council on 11 February with the adoption of its *conclusions on cyber diplomacy*[38], as a response to the increase in the number of cyber-attacks and the deadlock in international negotiations on international law and state responsible behaviour in cyberspace.[39] These conclusions constitute an undoubted 'reference' since then, both for guiding the efforts of the EU and its Member States on cyber policy at the international level, and for proposing detailed objectives in response to foreign policy challenges in this area[40]. The conclusions also constituted the first EU official document to use the term cyber diplomacy as such,[41] and marked "the beginning of a more proactive role of the EU in international cyberspace policymaking". [42]

Paper, Chatham House, The Royal Institute of International Affairs, (2019); K. bannelier, and T. christakis, t. "Cyber-Attacks Prevention-Reactions: The Role of States and Private Actors", *Les Cahiers de la Revue Défense Nationale*, 2017, or o. gross "Legal Obligations of States Directly Affected by Cyber-Incidents", Cornell International Law Journal, vol. 48 (2015) pp. 1-38.

[32] Group of Governmental Experts on Advances in Information and Telecommunications in the Context of International Security, 22 July 2015 (A/70/174).

[33] See in this respect C. gutierrez espada, C., *La Responsabilidad Internacional por el uso de la fuerza en el ciberespacio*, Aranzadi, Cizur Menor, 2020, in particular Chapter 1, section III, para 7, or c. gutierrez espada, "La legítima defensa y el ciberespacio", Comares, 2020, para 22.

[34] JOIN(2013) 1 final, cit, p. 17.

[35] JOIN(2013) 1 final, cit. In particular, the strategy included, among the principles of European cybersecurity (paragraph 1.2), the protection of fundamental rights, freedom of expression, personal data and privacy, or democratic and effective multilateral governance.

[36] EU Action Plan for Human Rights and Democracy, under the EU Strategic Framework on Human Rights and Democracy (Council Conclusions on Human Rights and Democracy, Brussels, 25 June 2012, 11855/12, Annex III).

[37] Id. In particular see action number 24 of the EU Action Plan.

[38] Council Conclusions on Cyber Diplomacy, CYBER 5 RELEX 114 JAIEX 6 TELECOM 32 COPS 42, Brussels, 11 February 2015.

[39] See to this extent Y. miadzvetskaya, and R.A. wessel, "The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox", European Papers, 2022, forthcoming, at page 15.

[40] C. Heinl, «Aperçu des stratégies, politiques et concepts actuels de l'Union européenne en matière de cyber», Observatoire Fic.com, 7 May 2019. As the author states "These Council conclusions are now considered as a reference, both to guide the EU's collective cyber policy efforts at the international level and to propose more detailed objectives in response to foreign policy challenges", available at: https://observatoire-fic.com/strategies-politiques-cyber-union-europeenne/

[41] A. barrinha, and T. renard, "Cyber-diplomacy: the making of an international society in the digital age", Global Affairs, 3:4-5, 2017, 353-364, at p. 359: "the European Union's member states adopted Council Conclusions on Cyber Diplomacy in 2015 - the first time the term "cyber-diplomacy" was used as such in an official government document".

[42] T. Renard, "EU cyber partnerships: Assessing the EU strategic partnerships with third countries in the cyber domain", European Politics and Society, 2018, 19(3):1-17, at p. 5.

20. In the 2015 conclusions the Council described the main content of cyber diplomacy as follows "cyberspace issues, in particular cyber security, the promotion and protection of human rights in cyberspace, the application of existing international law, rule of law and norms of behaviour in cyberspace, Internet governance, the digital economy, cyber capacity building and development, and strategic cyber relations offer significant opportunities, but also pose continuously evolving challenges for EU external policies, including the Common Foreign and Security Policy"[43]. In other words, cyber diplomacy deals with the regulation of cyberspace, the multilateral agenda linked to cyberspace challenges, and is clearly distinct from strategic communication or public diplomacy. In particular, EU cyber diplomacy focuses on issues such as international negotiations on cybersecurity, the fight against cybercrime, building trust and confidence in the Internet, Internet governance, or the promotion of fundamental rights and freedoms in cyberspace.[44]

21. The conclusions also underlined that the EU and its Member States should address the cross-cutting and multi-faceted issues mentioned above through a coherent international policy for cyberspace, an objective that was already explicitly mentioned in the 2013 cybersecurity strategy as one of the five priority areas for EU action, as discussed above[45].

22. The conclusions structured the aims of cyber diplomacy around six strategic objectives, namely: (i) Promotion and Protection of Human Rights in Cyberspace; (ii) Norms of behaviour and application of existing international law in the field of international security; (iii) Internet Governance; (iv) Enhancing competitiveness and the prosperity of the EU; (v) Cyber capacity building and development; and (vi) Strategic engagement with key partners and international organisations.

23. In short, the conclusions underlined the need to set priorities for the Union and its Member States in cyber issues, recognising that the strategy to address cyberspace risks goes beyond a legal or political response, requiring also joint and decisive diplomatic action to prevent conflicts, counter cybersecurity threats, and provide stability and coherence to the EU's international relations in this field. In this respect, as noted, the need for coherence is particularly evident in cyberspace policy, and especially in cybersecurity, where internal and external policies, civilian and military, public and private aspects converge, and where national, European and global spaces are blurred[46] .

24. Subsequently, the 2016 Global Strategy for the European Union's Foreign and Security Policy, endorsed the Union's efforts on cyber diplomacy. As stated in the Global Strategy, "We will engage in cyber diplomacy and capacity building with our partners, and seek agreements on responsible state behaviour in cyberspace based on existing international law. We will support multilateral digital governance and a global cooperation framework on cybersecurity, respecting the free flow of information.[47]

[43] Council conclusions on e-diplomacy, cit., Annex, p. 2.

[44] See also for the concept and content of cyber diplomacy A. Kasper, A-M. Osula and A Molnár, "EU cybersecurity and cyber diplomacy", IDP: revista de Internet, derecho y política = revista d'Internet, dret i política, Nº. Extra 34, 2021, pp. 1-15, at pp. 3-5.

[45] JOIN(2013) 1 final, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "EU Cybersecurity Strategy: Open, Secure and Safe Cyberspace", p. 16.

[46] H. Carrapico / A. Barrinha, "The EU as a Coherent (Cyber)Security Actor?", Journal of Common Market Studies, Volume 55. Number 6, 2017, pp. 1254-1272, in particular at p. 1255 "the EU has made cybersecurity one of its main security priorities. Such prioritisation has been reflected not only at the level of new initiatives being proposed, but also in the idea that in order for the EU to be an effective cybersecurity actor it needs to be fully coherent. Cybersecurity questions a number of important dichotomies (internal/external, public/private, civilian/military) while, simultaneously, blurring the geographical distinctions between national, European and global levels".

[47] European Union, Shared Vision, Common Action: A Stronger Europe; A Global Strategy for the European Union's Foreign and Security Policy (Brussels: European Union, June 2016), https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf.

25. In this context, the conclusions on cyber diplomacy were updated in 2017, in view of the increasing severity of cybersecurity threats in the European Union[48] . The Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), presented in June 2017, developed the principles of the "Non-paper" presented by the Dutch Council Presidency in 2016 under the title "*Developing a joint EU diplomatic response against coercive cyber* operations"[49].

26. In this respect, the Toolkit revealed the motivation of the Union's policy in this area by stating that communicating the possible consequences of a joint EU diplomatic response to malicious cyber activity would influence "the behaviour of potential aggressors in cyberspace, thus reinforcing the security of the EU and its Member States"[50]. In this regard, the assumption that potential aggressors in cyberspace have been deterred by the adoption of cyber diplomacy measures is questionable in light of the recent experience of the EU, as will be discussed below.

27. The Union's reinforced determination in preventing and responding to cyber-attacks is particularly manifest in the final part of the Council conclusions, concerning cyber diplomacy instruments, by recognising the possibility of adopting sanctions under the Common Foreign and Security Policy provisions in response to cyber-attacks. In the terms used by the Council "The EU affirms that measures within the Common Foreign and Security Policy, including, if necessary, restrictive measures, adopted under the relevant provisions of the Treaties, are suitable for a Framework for a joint EU diplomatic response to malicious cyber activities and should encourage cooperation, facilitate mitigation of immediate and long-term threats, and influence the behavior of potential aggressors in a long term"[51]. In this regard, as noted by Wessel, the broad wording of Article 24(1) TEU, namely that "the Union's competence in matters of common foreign and security policy shall cover all areas of foreign policy and all questions relating to the Union's security", allow for cyber diplomacy measures "to be taken using CFSP as a legal basis."[52]

28. Finally, the measures to be adopted were not set out in detail, although it was mentioned that they could be sanctions (restrictive measures), and also less drastic, such as the adoption of joint expressions of condemnation or reprobation of a given action by a State or non-state actor. In this regard, it is submitted that this type of measure, of a more diplomatic than sanctioning nature, appears only effective, or at least especially so, in relation to the conduct of State actors. However, as will be discussed below, many EU cyber diplomacy measures, and particularly the restrictive measures that can be adopted in the event of cyber-attacks, are directed at non-state actors.

29. The Cyber Diplomacy toolkit concluded by stating that the Union would continue to work on the development of the framework for a joint EU diplomatic response to malicious cyber activities, in particular by developing guidelines for the implementation of the toolkit[53] . These guidelines were adopted by the Political and Security Committee a few months later, namely in October 2017, in fulfilment of its functions to implement the policies agreed in this area under Article 38 TEU[54] .

30. The guidelines distinguished between five types of cyber diplomacy measures, which could be used independently, sequentially or in parallel in order to influence specific actors:

---

[48] Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), 7 June 2017, CYBER 91 RELEX 482 POLMIL 58 CFSP/CFSP 476.

[49] Non-paper: Developing a joint EU diplomatic response against coercive cyber operations-final revised text, Brussels, 19 May 2016, 5797/6/16 REV 6.

[50] Council Conclusions on a framework for a joint EU diplomatic response to malicious cyber activity, cit.

[51] Council Conclusions on a framework for a joint EU diplomatic response to malicious cyber activity, cit., p. 4

[52] See in this regard R.A. wessel, 'European Law and Cyberspace', in N. tsagourias and R. buchan (Eds.), *International Law and Cyberspace*, cit, at p. 501.

[53] Ibid.

[54] Implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities, Brussels, 9 October 2017, CYBER 142CFSP/PESC 855COPS 302RELEX 836.

— **Preventive measures**, in particular confidence-building measures supported by the EU, such as those developed in the framework of the OSCE, measures to raise awareness of EU policies, such as the EU's cyber dialogues with Brazil, China, India, Japan, the Republic of Korea and the United States, and measures adopted with the view of enhancing the capacity to prevent cyber-attacks in third states, particularly cyber capacity building, which can also be particularly appropriate to allow third states to be able to meet internationally agreed standards for the prevention of cyber-attacks.
— **Cooperative measures (between Member States)**, in particular cooperation is foreseen through EU-led political and thematic dialogues or demarches by EU delegations, such as facilitating the peaceful resolution of a conflict through the use of diplomatic channels of other Member States or the EU.[55]
— **Stability measures**, in particular the promotion of strategic communication (statements by the High Representative and on behalf of the EU Council, EU Council conclusions, diplomatic demarches by EU delegations, signaling through EU-led political and thematic dialogues...) to influence potential attackers by indicating the importance for the Union and its Member States of the security and integrity of cyberspace, and the potential consequences of malicious cyber activity.
— **Restrictive measures**, which are discussed in more detail in the following section; it is worth mentioning here that the guidelines envisaged, if necessary, the adoption of measures under the joint application of Articles 29 TEU and 215 TFEU in response to malicious activities, which have already been adopted and implemented as will be discussed below; and
— **Possible EU support to Member States' lawful responses**. The guidelines also foresaw the possibility for the EU to support individual or collective measures by Member States, which could not be taken in the framework of the CFSP, provided that they were taken in accordance with the international legal order. The types of measures that could be adopted in this regard could include countermeasures adopted by the State victim of a cyber-attack that can be regarded as an international wrongful act, the invocation of the self-defence, individual or collective under Article 51 of the UN Charter, or the application of the mutual defence clause under Article 42(7) TEU.

31. In light of the foregoing, cyber diplomacy measures include not only actions involving international actors but also measures concerning Member states only, highlighting the close interconnection of the internal and external dimensions of cybersecurity. Among the cyber diplomacy measures concerning international actors, two main types can be underlined for the purposes of analyzing the cooperation of the EU with international actors and the possible development of normative standards: (i) preventive measures and (ii) restrictive measures.

Preventive cyber diplomacy measures

32. In 2018 the Council adopted the EU External Cyber Capacity Building Guidelines, which underlined that the EU's core values and principles for cybersecurity, defined in the 2013 Cybersecurity Strategy, "should serve as the underlying framework for any external cyber capacity building action, to ensure that it: incorporates the understanding that the existing international law and norms apply in cyberspace; is rights-based and gender-sensitive by design, with safeguards to protect fundamental rights and freedoms; promotes the democratic and efficient multi-stakeholder internet governance model; supports the principles of open access to the internet for all, and does not undermine the integrity of infrastructure, hardware, software and services; adopts a shared responsibility approach that entails involvement and partnership across

[55] See in this regard A. bendiek, "The EU as a Force for Peace in International Cyber Diplomacy", SWP Comment, NO. 19 April 2018, German Institute for International and Security Affairs, 2018, pp. 57-71 at p. 60 "Cyber diplomacy -as opposed to overall cyber defense- offers the potential for conflict de-escalation and thus for developing a force for peace."

public authorities, [and] the private sector and citizens and promotes international cooperation."[56]More recently, the Commission stressed that the EU has "a core interest in actively contributing to discussions on the future governance of cyberspace. Therefore, in order to better promote its position and disseminate its core values, the EU should engage via various outreach and capacity building activities with wide range of stakeholders, both with internal and external, governmental and non-governmental."[57]

33. In this context, the EU has developed strategic partnerships with a cyber dimension with a number of international partners. In particular, the EU has established formal Cyber Dialogues for exchanging lessons learnt, improving coordination and agreeing on priority actions. These Cyber Dialogues are coordinated by the EU External Action Service and have been formally entered into with China, Japan, Republic of Korea, Brazil, India, Ukraine and the United States, the latter relationship being by far the closest and most developed in this field. In addition, the EU is also determined to work with regional organisations in this area, as evidenced by the cooperation envisaged with the African Union, West African countries, or ASEAN,[58] in addition to the close cooperation established with the Council of Europe in the area of cybercrime.

34. Renard has referred in this context to 'cyber partnerships', defined as 'a form of cooperation between two international actors on cyber-related issues, based on shared interests and objectives, and underpinned by mutually agreed norms and mechanisms. As such, they are an advanced form of 'cyber international relations' beyond mere interactions, with the inclusion of a strategic and diplomatic dimension. '[59] As this author notes, EU's cyber partnerships have developed as a result of two main developments: the EU's ambition to become a global strategic actor and the incremental shaping of a European agenda on cyber issues.

35. In this regard, the EU has been successful in obtaining the support of international partners for joint cooperation in this field, which entails recognition of the EU as a relevant actor in this area.[60] For example, the Joint statement between the EU and South Korea, adopted in 2015, notes that "The Leaders emphasized the importance of ensuring the openness and security of cyberspace for it to continue being a driving force for the freedom, prosperity and economic growth of mankind. They agreed to increase bilateral cooperation on cyberspace as well as to strengthen the global partnership in response to threats arising from cyberspace." [61]More recently, a May 2022 Joint Statement between the EU and Canada noted that the parties pledge "to continue to advance the application of international law, norms of responsible state behavior, confidence building measures and capacity-building initiatives, including in the UN through the establishment of the UN Programme of Action to Advance Responsible State Behaviour in Cyberspace."[62]

36. The international role of the EU in this context has also been recognized in multilateral fora, notably in UN discussions related to cyber issues, where participants underlined "the moderating role of the EU in intergovernmental processes, that it should act as a force for good in the world and in the promotion of a rules-based and human rights-based cyberspace. The EU could also play a lead role in discussions related to the protection of privacy of data and undue intervention on democratic institutions."[63]

---

[56] EU External Cyber Capacity Building Guidelines, Brussels, 26 June 2018, 10496/18, at p. 7.

[57] European Commission, 2020, Annex 9 of the Commission Implementing Decision on the 2020 Annual Action programme for the Partnership Instrument, Action Document for EU Cyber Diplomacy Support Initiative, at p. 2.

[58] See in this regard, for example, the Joint statement of the 6th European Union - African Union Summit: A Joint Vision for 2030, 18 February 2022, the West African Response on Cybersecurity and Fight Against Cybercrime (OCWAR - C) project, or the ASEAN-EU Statement on Cybersecurity Cooperation of August 1st 2019.

[59] T. renard, "EU cyber partnerships: Assessing the EU strategic partnerships with third countries in the cyber domain", cit., at p. 4.

[60] Id., p. 8.

[61] Joint Press Statement, 8th Republic of Korea-EU Summit, Seoul, 15 September 2015.

[62] Joint declaration following the third EU-Canada Joint Ministerial Committee meeting, 16 May 2022.

[63] Regional Consultations series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cy-

37. In relation to the foregoing, a recent report stressed the increasing importance of cyber capacity building as a mechanism for the EU's engagement with its partners. The authors underlined in this regard that cyber capacity building occupies a central place in major international fora, including at the UN, and that "partner countries and regional organisations also seem to be increasingly interested in working with the EU, either through traditional capacity building partnerships or to address cyber-related issues broadly, as the requests for starting new official cyber dialogues and having peer-to-peer exchanges would indicate".[64]

38. Indeed, preventive measures, and particularly cooperation in capacity building with international partners, are nowadays an important cyber diplomacy tool. A relevant example of this dimension of cyber capacity building as a way to promote EU values and normative ambitions is represented by the fact that the EU is offering some of its capacity building projects only to countries that have been invited to accede or have signed or ratified the Budapest Convention on Cybercrime. To this extent, as reportedly noted by some EU officials, "EU's cyber capacity building cannot be value-free, as the EU's core values and principles on fundamental rights, democracy and the rule of law also translate to cyberspace".[65]

39. To conclude, there is more to preventive measures that meets the eye. As it has been held, they not only build trust among partners and foster cooperation, but also reinforce the role of the EU as a global actor in this field, and strengthen global governance.[66] In addition, through Cyber Dialogues and capacity building the EU also displays a transformative power in jurisdictions beyond the EU, for instance by incentivizing the adoption normative standards such as the Budapest Convention on Cybercrime.

Restrictive measures

40. In relation to restrictive measures, the growing threat posed by cyber-attacks prompted an increasingly determined reaction from the European Union, culminating in the adoption and implementation of a legal framework of restrictive measures in response to cyber-attacks. This framework is composed of Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (hereinafter "the Decision")[67] and Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (hereinafter "the Regulation")[68] . The Decision was extended for one year in May 2020, for another year in 2021,[69] and most recently for three years, until 18 May 2025,[70] showing the EU's commitment to the framework created in 2019.

---

berspace in the Context of International Security, United Nations, 12 March 2019, p. 11 *in fine*. See for the reference A. Kasper and V. Vernygora, "The EU's cybersecurity: a strategic narrative of a cyber power or a confusing policy for a local common market?", cit, at p.58.

[64] R. Collett, and N. Barmpaliou, "International cyber capacity building: global trends and scenarios", EUISS, Luxembourg, 2021, p. 58.

[65] Id. 57.

[66] T. Renard, "EU cyber partnerships: Assessing the EU strategic partnerships with third countries in the cyber domain", cit., at p. 15.

[67] 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, OJ L 129I, 17.5.2019, p. 13/19.

[68] Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks that threaten the Union or its Member States, ST/7302/2019/INIT, OJ L 129I, 17.5.2019, p. 1/12.

[69] Council Decision (CFSP) 2020/651 of 14 May 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 153, 15.5.2020, p. 4-4; Council Decision (CFSP) 2021/796 of 17 May 2021 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 174I , 18.5.2021, p. 1-1.

[70] Council Decision (CFSP) 2022/754 of 16 May 2022 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 138, 17.5.2022, p. 16-16.

41. The adoption of a framework of restrictive measures in response to cyber-attacks, the second adopted by an international actor after the similar system approved in 2015 in the US[71], shows the European Union's resolve to play a significant role in shaping the digital environment worldwide. At the same time, the EU aims to stand out as an international actor committed to multilateralism, in particular to the respect of existing international law applicable to cyberspace and to the norms of responsible behaviour adopted in different international fora, such as the OSCE, as the Union has repeatedly affirmed, for example in the Declaration by the High Representative on behalf of the EU on respect for the rules-based order in cyberspace of 12 April 2019[72] .

42. The Decision and the Regulation aim to prevent and counter cyber-attacks that have a significant impact and constitute an external threat to the Union or its Member States, and are therefore consistent with the defence of the values, fundamental interests, security, independence, and integrity of the Union provided for in Article 21(2)(a) TEU. Furthermore, and only to the extent that they are deemed necessary for the fulfilment of the objectives of the CFSP provided for in Article 21 TEU, the Decision and the Regulation allow for restrictive measures in response to cyber-attacks - in this case attempted cyber-attacks are not envisaged - with a significant effect against third states or international organisations.

43. The restrictive measures that the Council may impose are set out in Articles 4 and 5 of the 2019 Decision. These measures consist of restrictions on entry or transit and/or the freezing of funds and economic resources, the former applying only to natural persons and the latter to natural or legal persons, entities or bodies. In addition, it is prohibited to make funds available, directly or indirectly, to the sanctioned persons and entities or bodies.

44. In particular, Article 4 makes it possible to prevent the entry into or transit through the territory of the Member States of natural persons responsible for cyber-attacks or attempted cyber-attacks, natural persons assisting the above or otherwise involved "in cyber-attacks or attempted cyber-attacks, including by planning, preparing, participating in, directing, assisting or encouraging such attacks, or facilitating them whether by action or omission"[73], or natural persons associated with the above.

45. The natural persons against whom these restrictive measures are directed must be listed in the Annex to the Decision. Article 4 also provides for exceptions to the adoption of the measures provided for therein on the basis of international law, such as not obliging Member States to refuse entry into their territory to their own nationals, or not imposing restrictive measures on certain persons on the basis of a multilateral agreement conferring privileges and immunities.

46. Article 5 of Decision 2019/797 and Article 3 of Regulation 2019/796 provide for the freezing of all funds and economic resources belonging to, owned, held or controlled by "(a) natural or legal per-

[71] The cyber sanctions programme implemented by the Office of Foreign Assets Control (OFAC) officially began on 1 April 2015, when President Obama issued Executive Order (E.O.) 13694 and declared a national emergency to address the unusual and extraordinary threat to the national security, foreign policy and economy of the United States posed by the increasing prevalence and severity of malicious cyber activities originating from or directed by persons located, in whole or in substantial part, outside the United States. However, as early as January 2015, the US government had adopted sanctions against North Korea for the cyberattack against the SONY company carried out on 22 November 2014. Information on this framework can be found at the following link: https://www.treasury.gov/resource-center/sanctions/Programs/pages/cyber.aspx

[72] As this declaration states "In order to keep cyberspace open, stable and secure, the international community needs to increase its efforts to tackle malicious cyber activities, and guide its own use of ICTs by the application of existing international law in cyberspace, as well as through the adherence to the norms, rules and principles of responsible state behaviour as articulated in the cumulative reports from the UN Group of Governmental Experts in the field of Information and Communications Technologies (ICTs) in the Context of International Security (UNGGE). In this regard, states should not knowingly allow their territory to be used for malicious activities using ICTs as it is stated in the 2015 report of the UNGGE." The statement is available at the following link: https://www.consilium.europa.eu/es/press/press-releases/2019/04/12/declaration-by-the-high-representative-on-behalf-of-the-eu-on-respect-for-the-rules-based-order-in-cyberspace/

[73] *Id.,* Article 4.1(b).

sons, entities or bodies that are responsible for cyber-attacks or attempted cyber-attacks; (b) natural or legal persons, entities or bodies that provide financial, technical or material support for or are otherwise involved in cyber-attacks or attempted cyber-attacks, including by planning, preparing, participating in, directing, assisting or encouraging such attacks, or facilitating them whether by action or omission; (c) natural or legal persons, entities or bodies associated with the natural or legal persons, entities or bodies covered by points (a) and (b)". The second paragraph of Article 5 also establishes the obligation not to make funds or economic resources available, directly or indirectly, to or for the benefit of the natural or legal persons, entities or bodies referred to.

47. In any case, both natural and legal persons against whom restrictive measures are taken on the basis of the Decision and/or the Regulation must be listed in Annex I provided for this purpose in both pieces of secondary legislation[74].

48. In this regard, according to Article 6(1) of the Decision, the Council, acting by unanimity upon a proposal from a Member State or from the High Representative of the Union for Foreign Affairs and Security Policy, shall establish and amend the list set out in the Annex. For its part, the Regulation does not specify the procedure for adopting the decision to include natural or legal persons in its Annex I, although it does state in its preamble that the Council shall exercise the power to establish and amend the list, "in order to ensure consistency with the process of establishing, amending and reviewing the Annex to Decision (CFSP) 2019/797"[75] , and article 3.3 thereof states that Annex I shall include, "as defined by the Council in accordance with Article 5(1) of Decision (CFSP) 2019/797" the natural or legal persons held liable.

49. Natural and legal persons listed in the annexes to the Decision and the Regulation may submit observations for the Council to reconsider their inclusion. The Council will have to do so if substantial observations or evidence is submitted, as it has already done with the above-mentioned decision of November 2020. This follows from the requirements of the rights of defence and effective judicial protection, as recognised by Articles 47 and 48 of the EU Charter of Fundamental Rights, and from the case law of the EU Courts.[76]

50. By decision and regulation adopted on 30 July 2020,[77] , the Council imposed restrictive measures against six individuals and three entities from Russia, North Korea and China - thus avoiding singling out a state only - for their involvement in the attempted cyber-attack against the Organisation for the Prohibition of Chemical Weapons and in the cyber-attacks publicly known as WannaCry, NotPetya and Operation Cloud Hopper.

51. In connection with the above, the Council imposed further restrictive measures on 22 October 2020 on two Russian nationals, including the current head of the Main Command of the Defence General Staff of the Armed Forces of the Russian Federation (GU/GRU), and a Russian official body, the 85th Main Centre for Special Services (GTsSS) of the Main Command of the Defence Staff of the Armed Forces of the Russian Federation (GU/GRU), for their involvement in the cyber-attack against

[74] In this regard, as stated in Article 7(2) of the Decision and Article 14(2) of the Regulation, the "The Annex shall contain, where available, the information necessary to identify the natural or legal persons, entities or bodies concerned. With regard to natural persons, such information may include: names and aliases; date and place of birth; nationality; passport and identity card numbers; gender; address, if known; and function or profession. With regard to legal persons, entities or bodies, such information may include names, place and date of registration, registration number and place of business".

[75] Council Regulation (EU) 2019/796 of 17 May 2019, OJ L 129I, 17.5.2019, p. 1/12, preamble paragraph 4.

[76] See, for example, the judgment of the General Court of 12 December 2006 in Case T-228/02, Organisation des <Modjahedines du peuple d'Iran v Council> (ECLI:EU:T:2006:384).

[77] 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, OJ L 246, 30.7.2020, p. 12–17; 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, OJ L 246, 30.7.2020, p. 4–9.

the German Federal Parliament carried out in April and May 2015.[78] Subsequently, in November 2020 two listings of natural persons were amended following the receipt of updated information.[79]In this regard, the lack of new listings since October 2020, together with other factors such as "a lack of coordinated intelligence collection efforts, a focus on voluntary intelligence sharing, and a political process that likely undermines the creation of a common EU threat perception in cyberspace" have led some authors to conclude that the regime has failed to achieve its strategic aims and even to question whether the EU cyber sanctions regime is dead,[80]although, as mentioned before, the recent renewal of the framework for three years could point to the opposite direction.[81]

52. Finally, beyond the question of its effectiveness, the application of the framework of restrictive measures might raise, in our view, fundamental rights concerns, particularly in relation to the principle of legal certainty. In this respect, according to the case law of the European courts, the principle of legal certainty, which is a general principle of Union law, requires that legal rules be clear, precise and foreseeable as to their effects, in particular where they may have adverse consequences for individuals and companies.[82] However, the sanctions adopted in July and October 2020, under a restrictive measures regime adopted in May 2019, have been imposed in response to cyber-attacks, and an attempted cyber-attack, committed prior to the adoption of such a regime, namely in 2015, 2017 and 2018. The foreseeability requirement required by the case law, as well as by Article 49 of the EU Charter of Fundamental Rights, does not seem to be observed in those instances.

IV. The external dimension of EU cybersecurity and the 2020 Cybersecurity strategy

53. At the end of 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy published a new Cybersecurity Strategy "for the Digital Decade".[83] The new strategy set out "how the EU will shield its people, businesses and institutions from cyber threats, and how it will advance international cooperation and lead in securing a global and open Internet."[84] The Strategy identified three areas of EU action - (i) resilience, technological sovereignty and leadership, (ii) building operational capacity to prevent, deter and respond, and (iii) advancing a global and open cyberspace.

54. Section 2.3 of the Strategy, entitled EU cyber diplomacy toolbox, underlined the need to tackle malicious cyber activities through an effective and comprehensive joint EU diplomatic response. For these purposes, it proposed the establishment of a Member States' EU cyber intelligence working group within the EU Intelligence and Situation Centre (INTCEN) to advance strategic intelligence cooperation on cyber threats and activities, a particularly important element for an effective prevention and response to cyber-attacks in our view. The Strategy also announced the future presentation by the High Representative of a proposal for the EU to further define its cyber deterrence posture, which would

[78] 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, OJ L 351I, 22.10.2020, p. 5/7; Council Implementing Regulation (EU) 2020/1536 of 22 October 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 351I, 22.10.2020, p. 1/4.

[79] Council Decision (CFSP) 2020/1748 of 20 November 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 393, 23.11.2020, p. 19-20.

[80] S. Soesanto, "After a Year of Silence, Are EU Cyber Sanctions Dead?", available at https://www.lawfareblog.com/after-year-silence-are-eu-cyber-sanctions-dead

[81] Council Decision (CFSP) 2022/754 of 16 May 2022 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 138, 17.5.2022, p. 16-16.

[82] See on individual sanctions, Judgment of the General Court of 16 July 2014, T-578/12, <National Iranian Oil Company v Council of the European Union>, EU:T:2014:678, paras 112-114.

[83] 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.

[84] Id., p. 4.

build on the work under the cyber diplomacy toolbox and contribute to responsible state behaviour and cooperation in cyberspace. The Council Conclusions on the development of the European Union's cyber posture were finally adopted in May 2022.[85]

55. These initiatives were further underlined in the Strategic Compass, approved by the Council in March 2022.[86] The Strategic Compass introduced a new Hybrid Toolbox and EU Hybrid Rapid Response Teams, enhanced the Cyber Diplomatic Toolbox and proposed, *inter alia*, the development of an EU toolbox to address and counter foreign information manipulation and interference. In this regard, it has been suggested that, instead of further reinforcing the existing Toolbox and creating others, the EU should focus "on improving retention of institutional expertise and flexible thematic implementation modules".[87]

56. The Strategy also mentioned the possibility of exploring qualified majority voting (QMV) for listings under the horizontal sanctions regime against cyber-attacks, which was related to the announcement of an update of the 2017 implementing guidelines of the cyber diplomacy toolbox, and the will to strengthen the cooperation with international partners, including NATO in order to advance the shared understanding of the threat landscape, develop cooperation mechanisms and identify cooperative diplomatic responses.[88] In this regard, the recently adopted NATO 2022 Strategic Concept also underlines the importance of the NATO-EU collaboration by holding that "The European Union is a unique and essential partner for NATO. NATO Allies and EU members share the same values. NATO and the EU play complementary, coherent and mutually reinforcing roles in supporting international peace and security."[89]

57. In relation to the foregoing, the idea of moving the adoption of sanctions to QMV is not new. President Juncker underlined the need to use QMV in foreign policy decisions in 2017,[90] and a Commission's communication subsequently suggested that "the Council consistently uses qualified majority voting for amending the listings of all EU sanctions regimes – including autonomous measures – in accordance with the procedures under Article 31(2) TEU (third indent)."[91]Similarly, President Von der Leyen encouraged Member States to move to QMV decisions concerning human rights and sanctions in her first State of the Union speech.[92] In this context, while recognizing that QMV would lead to a more

[85] Council conclusions on the development of the European Union's cyber posture, Brussels, 23 May 2022, 9364/22.

[86] A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security, Brussels, 21 March 2022, 7371/22, at p. 22: "We must also be able to swiftly and forcefully respond to cyberattacks, such as state-sponsored malicious cyber activities targeting critical infrastructure and ransomware attacks. To this end, we will reinforce our ability to identify and analyse cyberattacks in a coordinated manner. We will strengthen the EU Cyber Diplomacy Toolbox and make full use of all its instruments, including preventive measures and sanctions on external actors for malicious cyber activities against the Union and its Member States. We will contribute to the EU's Joint Cyber Unit to enhance joint situational awareness and cooperation between EU Institutions and Member States."

[87] See in this regard, S. blockmans, D. macchiarini crosson and Z. Paikin, "The EU's Strategic Compass: A guide to reverse strategic shrinkage?", CEPS Policy Insights No 2022-14 / March 2022, at p. 5.

[88] Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, cit. See in this regard also the May 2022 Cyber Posture: "EMPHASISES the need to further strengthen cyber cooperation with NATO through exercises, information sharing and exchanges between experts, including on capability development, capacity building for partners, and missions and operations, as well as on the applicability of international law and UN norms of responsible State behaviour in cyberspace, and possible coordinated responses to malicious cyber activities. "Council conclusions on the development of the European Union's cyber posture, Brussels, 23 May 2022, 9364/22, id. p. 16.

[89] NATO 2022 Strategic Concept, at point 43, available at https://www.nato.int/cps/en/natohq/news_197281.htm

[90] European Commission, State of the Union Address by President Juncker (Brussels 13 Sept. 2017): "I want our Union to become a stronger global actor. In order to have more weight in the world, we must be able to take foreign policy decisions quicker. This is why I want Member States to look at which foreign policy decisions could be moved from unanimity to qualified majority voting. The Treaty already provides for this, if all Member States agree to do it. We need qualified majority decisions in foreign policy if we are to work efficiently."

[91] Communication from the Commission to the European Council, the European Parliament and the Council *A stronger global actor: a more efficient decision-making for EU Common Foreign and Security Policy* COM/2018/647 final, p. 11.

[92] European Commission, State of the Union Address by President von der Leyen at the European Parliament Plenary (Brussels 16 Sept. 2020): "But what holds us back? Why are even simple statements on EU values delayed, watered down or held hostage for other motives? When Member States say Europe is too slow, I say to them be courageous and finally move to QMV – at least on human rights and sanctions implementation".

efficient and speedy decision-making process, some authors have noted that it might also have some disadvantages, for instance related to the lack of commitment of the countries that vote against a certain sensitive decision that is ultimately approved, which could decide to ignore it, even if this makes them liable to infringement proceedings.[93]

58. Additional response measures under the EU Cyber diplomacy Toolbox will also be explored in the revised implementing guidelines.[94] In this regard, the Cyber Posture requested the High Representative to identify possible EU joint responses to cyberattacks, including sanctions options.[95] The Cyber Posture also noted that the EU is committed to mobilise "all available tools, internal and external, to prevent, discourage, deter and respond to cyberattacks, implementing these in a swift, effective, gradual, targeted and sustained approach based on long-term strategic engagement".[96] These tools could arguably also include the invocation of the mutual defence and solidarity clauses, as discussed further below.

59. In relation to the third area of EU action, namely advancing a global and open cyberspace, the Strategy underlined that the EU should promote, together with international partners, a political model and vision of cyberspace grounded on key EU values such as the rule of law, human rights or fundamental freedoms. It also stressed the EU's intention to lead in defining and promoting international norms and standards.[97]

60. In this context, the Strategy noted that the EU would continue working with international partners to advance and promote a global, open, stable and secure cyberspace under international law, and particularly the United Nations Charter, and supporting the voluntary non-binding norms, rules and principles of responsible state behavior, as reflected in the 2010, 2013 and 2015 reports of the Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, endorsed by the General Assembly of the United Nations. [98]

61. Interestingly, the Strategy observed that "With the deterioration of an effective multilateral debate on international security in cyberspace, there is a clear need for the EU and Member States to take a more proactive stance in the discussions in the UN and other relevant international fora".[99] In this context, the Strategy underlined the EU's support to the Programme of Action to Advance Responsible State Behaviour in Cyberspace (PoA) a proposal initiated by France and Egypt and supported by the EU Member States, among others, which proposes, *inter alia,* to create a framework and a political commitment based on recommendations, norms and principles already agreed under the auspices of the UN.[100] The support to the PoA features also in the May 2022 Cyber Posture. [101]

62. In this regard, it is submitted that to be an effective normative power in this context the EU will have to show more unity and cohesion among the EU Member States' positions.[102] To this extent,

[93] The authors refer to the Council Decision on the refugee relocation quotas, adopted by QMV, as an example. K. pomorska and R.A. wessel, 'Qualified Majority Voting in CFSP: A Solution to the Wrong Problem?' (2021) 26(3) European Foreign Affairs Review 351-358, at pp. 354-355.

[94] A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security, cit.

[95] Council conclusions on the development of the European Union's cyber posture, Brussels, 23 May 2022, 9364/22, id. p. 16.

[96] Id., p. 18.

[97] Id., p. 19.

[98] Id. 20

[99] Ibid.

[100] Ibid. The proposal can be consulted at https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf.

[101] Council conclusions on the development of the European Union's cyber posture, Brussels, 23 May 2022, 9364/22, at p. 13.

[102] See in this regard also A. kasper, a-m. osula and A. molnár, "EU cybersecurity and cyber diplomacy", IDP: revista de Internet, derecho y política = revista d'Internet, dret i política, cit. at p. 7: "the Union needs to achieve greater coherence among Member States and translate the discussions into clear messages to be reflected to external partners."

as it has been held, "In the [UN] negotiations, European countries have given the impression that they are working independently from each other, although there is a willingness to adopt a common position nowadays [...] despite the adoption of the "Cyber Diplomacy Toolbox" by the European Union, some states have been more inclined to side with other coalitions and with non-European countries. This European inability to offer a unified voice has been reinforced by the fact that, during the adoption and negotiation of the previous [UN] resolutions, they have been portrayed as simply following the United States. That said, there is a genuine European willingness to act in a more united manner and to position itself as a major actor in international discussions."[103]

63. In this context, the Cyber Posture proposed the development of an "EU outreach approach on how to promote a global common understanding of the application of international law in cyberspace".[104] In this regard, while the EU has supported in many occasions the application of international law, and of the United Nations Charter, to cyberspace, it is less clear how exactly the EU envisages such application, that is, the precise contours of international law in cyberspace. The more precise formulation was, to our knowledge, given by the 2017 Cyber Diplomacy Toolkit implementing guidelines. The Council recognized in those guidelines that malicious cyber activity is liable to constitute 'an internationally wrongful act', and that the victim Member States may in that case and under certain conditions, lawfully resort to non-forcible and proportionate countermeasures.[105]

64. The Council added, in line with general international law, that countermeasures are individual, adopted by the victim Member States against another subject of international law. In the terms used by the implementing guidelines 'These countermeasures constitute actions directed at another State that is responsible for the internationally wrongful act, which would otherwise violate an obligation owed to that State. Such non-forcible countermeasures are conducted to compel or convince the latter to cease the malicious cyber activity, in compliance with its international obligations.'[106]

65. In addition, the implementing guidelines recognized that some cyberattacks may amount to 'armed attacks' under Article 51 of the UN Charter, and therefore give rise to individual or collective self-defence under the Charter. The Council added that, in such scenario, Member States of the EU could also resort to the mutual defence clauses enshrined in Article 42(7) TEU.[107] In this regard, the implementing guidelines do not clarify the "grave instances" under which a cyber-attack can be equated to the use of force and therefore give rise to self-defence under international law. Taking the influential Tallinn Manual 2.0 as reference, which the guidelines cite,[108] we can conclude that "Acts that injure or kill persons or physically damage or destroy objects are uses of force".[109]

[103] F. delerue, F. douzet and A. géry, "The geopolitical representations of international law in the international negotiations on the security and stability of cyberspace", Report No. 75, IRSEM/EU Cyber Direct, November 2020, pp. 20-21.

[104] Council conclusions on the development of the European Union's cyber posture, Brussels, 23 May 2022, 9364/22, at p. 15.

[105] Implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities, Brussels, 9 October 2017, *cit*., p. 9.

[106] Ibid.

[107] Id. page 10: 'In grave instances, malicious cyber activities could amount to a use of force or an armed attack within the meaning of the Charter of the United Nations. In this latter case, Member States may choose to exercise their inherent right of individual or collective self-defense as recognized in Article 51 of the Charter of the United Nations and in accordance with international law, including international humanitarian law. A Member State may also choose to invoke article 42 (7) TEU to call on other Member States to provide aid and assistance.'

[108] Id., page 3, footnote 5: 'Tallinn Manual 2.0 provides an example of an academic analysis of how existing international law could apply to cyber operations, including a list of possible measures for States that have been subject to an internationally wrongful act in the cyber domain'

[109] M.N. Schmitt, (general editor*), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, cit, Rule 69, comment 8, p. 333. See also Rule 71, comment 12, p. 342: "The case of cyber operations that do not result in injury, death, damage, or destruction, but that otherwise have extensive negative effects, remains unsettled".

66. In relation to the damage to objects, it could be further explained that the physical or economic damage must be significant. To this extent, as the French Ministry of Defence has clarified, a cyber-attack affecting critical infrastructures with major consequences, or which could paralyse entire sections of a country's activity, trigger technological or ecological disasters and cause numerous victims, would be similar to the use of conventional weapons, and could therefore be considered as an armed attack.[110] Fortunately, most cyber-attacks do not meet this threshold and, as it has been held, no cyber-attack has so far met the characteristics required to qualify as an armed attack.[111] These assertions find broad academic support.[112]

67. It is worth recalling in this regard that NATO accepted in 2014 that a grave cyber-attack may allow the invocation of Article 5 of the North Atlantic Treaty.[113]More recently, the 2022 NATO Strategic Concept, adopted in Madrid in June 2022, clearly states that "A single or cumulative set of malicious cyber activities; or hostile operations to, from, or within space; could reach the level of armed attack and could lead the North Atlantic Council to invoke Article 5 of the North Atlantic Treaty. We recognise the applicability of international law and will promote responsible behaviour in cyberspace and space. We will also boost the resilience of the space and cyber capabilities upon which we depend for our collective defence and security."[114]

68. More recently, the European Parliament has proposed to reinterpret this framework in light of the increased number and gravity of cyberattacks and hybrid threats. In particular, the European Parliament has advocated for a EU-led reinterpretation of international law which would include the adoption of collective countermeasures on a voluntary basis and the right for collective defence provided for in Article 42(7) TEU below the collective defence threshold mentioned above,[115]in what could be regarded as a manifestation of the EU strategic autonomy in this context. In this context, it is worth noting that the NATO 2022 Strategic Concept also foresees the possibility of applying Article 5 of the North Atlantic Treaty in the event of a hybrid operation against Allies and mentions the possibility of cooperating with the EU in this regard.[116] While the proposed suggestions hold the potential to make the

[110] Ministère des Armées. Republique Française, « Droit International appliqué aux opérations dans le cyberespace », 9 septembre 2019, available at www.defense.gouv.fr, pp. 1-18, p. 9 : 'Une cyberattaque pourrait être qualifiée d'agression armée dès lors qu'elle provoquerait des pertes humaines substantielles, ou des dommages physiques ou économiques considérables. Cela serait le cas d'une opération dans le cyberespace provoquant une déficience des infrastructures critique avec des conséquences significatives, ou susceptibles de paralyser des pans entiers de l'activité du pays, de déclencher des catastrophes technologiques ou écologiques et de faire de nombreuses victimes. Dans une telle hypothèse, les effets de cette opération seraient similaires à ceux qui résulteraient de l'utilisation d'armes classiques'.

[111] F. Delerue, *Cyber operations and international law*, Cambridge University Press, 2020, p. 461.

[112] See, *inter alia*, C. gutierrez espada, *De la legítima defensa y el ciberespacio*, *cit*, para 24.

[113] Wales Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 05 Sep. 2014: "Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber-attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis".

[114] NATO 2022 Strategic Concept, at point 25, available at https://www.nato.int/cps/en/natohq/news_197281.htm

[115] In the terms employed by the European Parliament "the EU is increasingly involved in hybrid conflicts with geopolitical adversaries; underlines that these acts are of a particularly destabilising and dangerous nature as they blur the lines between war and peace, destabilise democracies and show doubt in the minds of target populations; recalls that these attacks are by themselves often not serious enough to trigger Article 5 of the NATO Treaty or Article 42(7) TEU, though they have a cumulative strategic effect and cannot be effectively tackled through retorsions by the injured Member State; believes that the EU should therefore strive to find a solution to fill this legal vacuum by reinterpreting Article 42(7) TEU and Article 222 TFEU in such a way that would reserve the right for collective defence below the collective defence threshold and allow for collective countermeasures by EU Member States on a voluntary basis, and should work internationally with allies towards a similar solution at international level; underlines that this is the only effective means to counter the paralysis in reacting to hybrid threats and is an instrument to increase the costs for our adversaries." State of EU cyber defence capabilities European Parliament resolution of 7 October 2021 on the state of EU cyber defence capabilities (2020/2256(INI), P9_TA(2021)0412, point 32.

[116] NATO 2022 Strategic Concept, *cit*., at point 27: "We will invest in our ability to prepare for, deter, and defend against the coercive use of political, economic, energy, information and other hybrid tactics by states and nonstate actors. Hybrid operations against Allies could reach the level of armed attack and could lead the North Atlantic Council to invoke Article 5 of the

response of the EU and the Member States more effective, it could also be regarded as at odds with the EU's commitment under Article 3(5) TEU to contribute to the strict observance and the development of international law, including respect for the principles of the United Nations Charter.

69. In relation to the foregoing, unlike self-defence, which can be individual or collective, collective countermeasures are not currently accepted under international law. This was established by the International Court of Justice in the case of military and paramilitary activities in and against Nicaragua (1986),[117] and subsequent practice does not confirm the existence of a general rule of international law which would permit it.[118]

70. However, some EU Member States have publicly defended the possibility of adopting collective countermeasures. For instance, in the terms employed by the President of the Republic of Estonia in 2019: "Estonia is furthering the position that states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation. The countermeasures applied should follow the principle of proportionality and other principles established within the international customary law".[119]

71. In this context, the Strategy also stressed the need to integrate the cyber diplomacy toolbox in EU crisis mechanisms and noted in this context that 'the EU should reflect upon the interaction between the cyber diplomacy toolbox and the possible use of Article 42.7 TEU and Article 222 TFEU.'[120] To this extent, the Strategic Compass added that 'We will continue to conduct regular exercises to further strengthen our mutual assistance in case of an armed aggression, in accordance with Article 42(7) of the Treaty on European Union. This will comprise regular cyber exercises starting from 2022."[121] Similarly, the May 2022 Cyber Posture underlined "the need to invest in our mutual assistance under Article 42(7) of the Treaty on European Union as well as solidarity under Article 222 of the Treaty on the Functioning of the European Union, in particular through frequent exercises".[122]

72. As mentioned before, the possibility of invoking the mutual defence and solidarity clauses under Article 42(7) TEU and Article 222 TFEU in the event of a cyberattack is not a novelty. The EU Member States, through the Cyber defence policy framework, the European Commission, the European Parliament and the High Representative have accepted this possibility in the past.[123]The main innova-

North Atlantic Treaty. We will continue to support our partners to counter hybrid challenges and seek to maximise synergies with other relevant actors, such as the European Union."

[117] Judgment of 27 June 1986, <Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)> ICJ Reports/CIJ Reports 1986, p. 117, para. 249: "The acts of which Nicaragua is accused, even assuming them to have been established and imputable to that State, could only have justified proportionate counter-measures on the part of the State which had been the victim of these acts, namely El Salvador, Honduras or Costa Rica. They could not justify counter-measures taken by a third State, the United States, and particularly could not justify intervention involving the use of force".

[118] See in this regard C. Gutierrez Espada, *La Responsabilidad Internacional por el uso de la fuerza en el ciberespacio*, cit., in particular Chapter 3, paragraph 4, subparagraph 69.

[119] Speech by the President of the Republic of Estonia at the opening of CyCon 2019. The national position of Estonia, first expressed in the Speech of the President at CyCon can be consulted at https://cyberlaw.ccdcoe.org/wiki/National_position_of_Estonia_(2019)

[120] Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, cit. p. 17.

[121] A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security, cit. at p. 20.

[122] Council conclusions on the development of the European Union's cyber posture, Brussels, 23 May 2022, 9364/22, at p. 11: It also added that "In this framework, STRESSES the need to work further on the provision and coordination of bilateral civilian and/or military support, including by exploring possible support provided by the EU upon an explicit request from Member States, and on identifying appropriate response measures, including through developing a coordinated communication strategy, in the context of the implementation of Article 42(7). NOTES that this should also include exploring the links with existing EU crisis management mechanisms and the EU Civil Protection Mechanism. "

[123] See, inter alia, for the solidarity clause: the 2013 EU Cybersecurity Strategy: an Open, Safe and Secure Cyberspace, JOIN/2013/01 final, p. 21; the Resilience, Deterrence and Defence: Building strong cybersecurity for the EU JOIN/2017/0450

tion is the proclaimed commitment to make these clauses fully operational in the cyber context through frequent exercises which combine cyber diplomacy, cyberdefence and crisis management mechanisms in order to better prepare the EU and its Member States to jointly mitigate the effects of a serious cyber-attack and to be able to respond to it effectively.

73. In relation to the foregoing, in addition to the possible adoption of voluntary collective countermeasures and the reinterpretation of Article 42(7) TEU and Article 222 TFEU, the EU could also contribute to the development of international law in this context by reinforcing the mandatory character of the due diligence principle, a principle already mentioned by the International Court of Justice in the *Corfu Channel* case, and whose origins can be traced back to the 1872 Alabama case.[124]

74. According to this principle, every State has the 'obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States".[125] This principle is applicable to cyberspace, as the Tallinn Manual 2.0 confirms: "A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States".[126]

75. As to its content, this principle imposes on States an obligation of conduct and not of result, as the International Court of Justice ruled in the *Genocide Convention* case.[127]In this regard, for instance, the actions adopted by the EU Member States under the Network and Information Security Directive and General Data Protection Regulation could serve as an example of possible measures that can be adopted to prevent and mitigate the effects of cyber-attacks.[128] In this regard, as it has been held, "the internal focus and reduction of vulnerabilities internally and building resilience at the level of Member States needs to be an integral part of the EU's cyber diplomacy."[129]

---

final, or the European Parliament resolution of 22 November 2012 on the EU's mutual defence and solidarity clauses: political and operational dimensions (2012/2223(INI)), whereas H. See also J. Rehrl, *Handbook on Cybersecurity The Common Security and Defence Policy of the European Union*, Publication of the Federal Ministry of Defence of the Republic of Austria, 2018, p. 239: "The need to respond to a particularly serious cyber incident or attack could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause". Regarding the mutual defense clause see, inter alia, the EU Cyber Defence Policy Framework adopted by the Council (14413/18, Brussels, 2018), p. 9, or the Implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities, Brussels, 9 October 2017, cit., p. 10.

[124] Alabama claims of the United States of America against Great Britain (1872) 24 RIAA 125, 129-131, in particular in p. 129: "And whereas the "due diligence" referred to in the first and third of the said rules ought to be exercised by neutral governments in exact proportion to the risks to which either of the belligerents may be exposed, from a failure to fulfil the obligations of neutrality on their part".

[125] Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania) (Judgment on the merits) [1949] ICJ Reports 4, 22.

[126] M.N. schmitt (general editor), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, cit.*, Rule 6, p. 30.

[127] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (BOSNIA AND HERZEGOVINA v. SERBIA AND MONTENEGRO), Judgment of 26 February 2007, p. 221, para. 430.: "Secondly, it is clear that the obligation in question is one of con-duct and not one of result, in the sense that a State cannot be under an obligation to succeed, whatever the circumstances, in preventing the com-mission of genocide : the obligation of States parties is rather to employ all means reasonably available to them, so as to prevent genocide so far as possible. A State does not incur responsibility simply because the desired result is not achieved ; responsibility is however incurred if the State manifestly failed to take all measures to prevent genocide which were within its power, and which might have contributed to preventing the genocide. In this area the notion of "due diligence", which calls for an assessment *in concreto*, is of critical importance".

[128] See in this regard also F. delerue, J. kulesza and P. pawlak, "The application of international law in cyberspace: is there a European way?", EU Cyber Direct, available at https://eucyberdirect.eu/research/the-application-of-international-law-in-cyberspace-is-there-a-european-way: "due diligence has become a substantial element of recent EU lawmaking, in particular through the Network and Information Security (NIS) Directive and General Data Protection Regulation (GDPR). Both documents introduce the flexible blueprint of good community practice as the standard for securing crucial data and infrastructures."

[129] A. Kasper/ A-M. Osula/ A. Molnár, "EU cybersecurity and cyber diplomacy", IDP: revista de Internet, derecho y política = revista d'Internet, dret i política, cit., at p. 11.

76. However, even though the due diligence principle is a "well-established rule of international law",[130] it is disputed by several major cyber powers, including Russia, China, the United States and the United Kingdom, which "appear hesitant to accept or even reject the legally binding nature of the due diligence obligation. "However, numerous others, including France, Germany, Finland, the Netherlands and Spain, recognise due diligence as an international law rule."[131]

77. These discrepancies among states could explain the (diluted) version of the principle included in the 2015 report of the UN Group of Governmental Experts on Advances in Information and Telecommunications in the Context of International Security, which provides, seemingly more as a recommendation than as an obligation, that States "should not" knowingly allow their territory to be used by non-state actors for such purposes,[132] a wording also included in UN Resolution 73/266 of 22 December 2018 (adopted with 138 States voting in favour). This formula was reproduced by the Council conclusions adopted on 16 April 2018 on malicious cyber activities,[133]and a reference to these conclusions and to the 2015 UN Group Report can also be found in the 2019 Decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States.[134]

78. In relation to the foregoing, the United Kingdom has recently referred to the formula employed by the 2015 UN report to reject the mandatory character of the due diligence principle by stating that "the fact that States have referred to this as a non-binding norm indicates that there is not yet State practice sufficient to establish a specific customary international law rule of 'due diligence' applicable to activities in cyberspace."[135] In this regard, as mentioned before, the mandatory nature of the due diligence principle has already been recognized by the International Court of Justice and it does not seem necessary in our view to devise a specific version of the principle narrowly limited to activities in cyberspace.

79. More recently, in the context of the coronavirus pandemic, the High Representative Borrell has referred to the principle of due diligence expressively,[136] and this statement has been quoted also by EU representatives before the UN. In particular, it has been held on behalf of the EU that "the EU and its Member States have called upon all UN Member States to exercise due diligence and take appropriate actions against actors conducting malicious activities from their territories, consistent with international law and the universally agreed norms of responsible State behavior."[137]

80. In this context, it is submitted that the EU could play a positive role for the observance and development of international law, in keeping with Articles 3(5) and 21 TEU, by contributing to conso-

[130] M.J. Cervell Hortal, *La legítima defensa en el derecho internacional contemporáneo: (nuevos tiempos, nuevos actores, nuevos retos)*, Tirant lo Blanch, Valencia, 2017, p. 128.

[131] J. Rehrl, *Handbook on Cybersecurity The Common Security and Defence Policy of the European Union*, cit., p. 31.

[132] See 2015 Group of Experts report (UN A/70/174), paragraph 13(c): "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs."

[133] Council conclusions on malicious cyber activities, Brussels, 16 April 2018 7925/18, p. 3.

[134] Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, *cit.,* paragraph 4 of preamble.

[135] A/76/136, Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution, 13 July 2021, contribution of the United Kingdom of Great Britain and Northern Ireland, page 117, point 12.

[136] Council of the European Union, 'Declaration by the High Representative Josep Borrell, on behalf of the European Union, on malicious cyber activities exploiting the coronavirus pandemic', 20 April 2020, available at https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/

[137] See the Statement on behalf of the European Union by Mr. Pawel Herczynski, Managing Director for CSDP and Crisis Response, EEAS, available at https://vm.ee/sites/default/files/Estonia_for_UN/20_05_22_arria_cyber_eu_statement_as_delivered_unread_paras.pdf See for this reference T., Dias & A. Coco, "Cyber due diligence in international law", p. 7, available at https://www.elac.ox.ac.uk/wp-content/uploads/2022/03/finalreport-bsg-elac-cyberduediligenceininternationallawpdf.pdf

lidate the principle of due diligence in this context as a mandatory rule of international law, in line with the Tallinn Manual,[138] and by clarifying its concrete practical application in light of existing international law, including international humanitarian law. In this regard, as it has recently been held "in debates about 'cyber due diligence', the controversial existence of a general principle or a cyber-specific rule of due diligence should not be presented as an alternative to a legal vacuum. This is because international law already provides more than meets the eye: a patchwork of due diligence duties that, together, require states to do their best to prevent, halt and respond to a wide range of online harms."[139]

81. In addition, the EU cyber-sanctions regime might be appropriate to signal cyber conduct that the EU (and other international actors that support the sanctions) considers unacceptable under international law. This could contribute to the development of international law, for instance by providing content to the discussions of the proposed UN convention on cybercrime, and to reinforcing the abovementioned due diligence principle, in particular by pointing to some States that their territory is being used for malicious cyber conduct that they should aim to halt and prevent. To this extent, as it has been held, the strength and main potential of the regime lies in its contribution to the development of international norms about the cyberspace, distinguishing, for example, an unlawful cyberattack like the one on the Bundestag, due to its scope and significance, from traditional intelligence gathering by States.[140]

82. However, the compatibility of the current EU cyber-sanctions regime with international law has also been questioned for a number of reasons, and particularly in light of the lack of internationally agreed obligations regulating behavior in cyberspace and the lack of attribution of cyberattacks to a State under the rules of state responsibility.[141]In this regard, the lack of attribution to specific international actors on which the framework is based may also significantly limit its purported deterrence effect.

83. In relation to the foregoing, as it has been held: "the EU relies on its cyber-sanctions regime to forge deterrence but it lacks the courage to attribute any cyber-operation to a potential state perpetrator, out of fear of political, reputational and economic costs and of escalating retaliation. Since "sanctions in the cyber-domain are more likely to deter states, but are less likely to deter individuals from acting in the name of states", how can this deterrence be effective if the EU does not take responsibility?"[142] In a similar vein, some authors have noted that travel bans and asset freezes do not directly impede an actor's ability to carry out a cyberattack.[143]

84. Indeed, the 2019 Council Decision concerning restrictive measures against cyberattacks recognizes, as did the Cyber diplomacy Toolkit and the implementation guidelines, that "Targeted restrictive measures should be differentiated from the attribution of responsibility for cyber-attacks to a third State. The application of targeted restrictive measures does not amount to such attribution, which is a sovereign political decision taken on a case-by-case basis. Every Member State is free to make its own determination with respect to the attribution of cyber-attacks to a third State.".[144] More recently, the

[138] M.N. Schmitt (general editor), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, cit., Rule 6, p. 30: "A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States".

[139] T. Dias / A. Coco, "Cyber due diligence in international law·, cit., pp. 163-164.

[140] S. Pantin Urdaneta, "EU Cyber sanctions and Cyber norms", in directionsblog.eu, available at https://directionsblog.eu/eu-cyber-sanctions-and-cyber-norms/

[141] I. Bogdanova/ M. vásquez Callo-Müller, "Unilateral Cyber Sanctions: Between Questioned Legality and Normative Value", Vanderbilt Journal of Transnational Law, Vol. 54, No. 4, 2021, Available at SSRN: https://ssrn.com/abstract=3976261, at page 943.

[142] C. Pâris, "Guardian of the Galaxy? Assessing the European Union's International Actorness in Cyberspace" College of Europe EU Diplomacy Paper 1/2021, pp. 1-38, at p. 29.

[143] S. Pantin Urdaneta, "EU Cyber sanctions and Cyber norms", cit., available at https://directionsblog.eu/eu-cyber-sanctions-and-cyber-norms/

[144] Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, *cit.,* paragraph 9 of preamble.

Strategic Compass also reminds, in the context of the attribution of hybrid attacks, that the "attribution is a sovereign national prerogative".[145]

85. In this regard, while the decision to impute responsibility for conduct is, in principle, a matter for States, including EU member states, this decision is not entirely free or "sovereign". This follows from the fact that many of the provisions, and in particular articles 4 to 11, of the Draft Articles on Responsibility of States for internationally wrongful acts adopted by the International Law Commission (ILC) in the summer of 2001, and taken note of by the UN General Assembly in its resolution 56/83 of 12 December 2001, are widely accepted as customary international law.[146] In this regard, the G7, at its 2017 Lucca meeting, underlined the customary nature of the rules on international liability, in particular those relating to imputation of liability[147].

86. In practice, it may be difficult in some instances to consider that there is no imputation, albeit indirectly,[148] on the part of EU Member States, as well as on the part of the Union itself, when adopting restrictive measures. In this regard, the restrictive measures adopted by the Union on 30 July 2020 targeted, *inter alia*, members of the Russian military intelligence service (GU/GRU), and official entities of that country, namely the Main Centre for Special Technologies (GTsST) of the Main Command of the Defence Staff of the Armed Forces of the Russian Federation (GU/GRU) and the legal framework itself foresees, as mentioned before, the possibility of imposing sanctions on persons that benefit from privileges and immunities under a multilateral agreement. In this context, it may not be surprising that the Russian Foreign Ministry responded to the adoption of these measures with a harsh communiqué in which it referred to them as "absolutely illegal in the context of international law",[149] and announced possible measures in response to their adoption, which entails an undesirable risk of escalation, heightened by the support that the measures adopted by the EU received from "like-minded" states such as the US, Canada and Norway, as well as from candidate and potential candidate countries.[150]

87. The Strategy also expressed the EU's support to third countries that wish to accede to the Council of Europe Budapest Convention on Cybercrime, and cautioned against the risks of division and slow down associated with the initiative for a new legal instrument on cybercrime at UN level,[151] boldly adding

[145] A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security, Brussels, 21 March 2022, 7371/22, at p. 22.

[146] See in this regard C. Gutiérrez Espada/ M.J. Cervell Hortal, *El Derecho Internacional en la encrucijada (Curso general de derecho internacional público)*, Editorial Trotta, 4.ª edición, 2017, p. 450 and by the same authors, *Introducción al Sistema Jurídico Internacional y de la Unión Europea*, Diego Marín Editores, Murcia, 2019, p. 81. See also t. Bruner, "States in Cyber-Space: Perspectives of Responsibility Beyond Attribution", European Consortium for Political Research (2014) available at: https://ecpr.eu/Events/PaperDetails.aspx?PaperID=17116&EventID=13.

[147] G7 Declaration on responsible states behavior in cyberspace Lucca, 11 Abril 2017, p. 2: "We note that the customary international law of State responsibility supplies the standards for attributing acts to States, which can be applicable to activities in cyberspace. In this respect, States cannot escape legal responsibility for internationally wrongful cyber acts by perpetrating them through proxies. When attributing an internationally wrongful act to another State, or when taking action in response, a State must act in accordance with international law. In this context, a State assesses the facts and is free to make its own determination in accordance with international law with respect to attribution of a cyber-act to another State".

[148] See in this regard Y. miadzvetskaya and R.A. wessel, "The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox", European Papers, 2022, forthcoming, at page 23: "We would argue that individual listings under the cyber-sanctions framework could be compared to the indirect attribution of responsibility to States since all actors sanctioned have a clear connection with a specific State."

[149] The Russian communiqué can be consulted at https://russiaeu.mid.ru/en/press-centre/news/comment_by_the_information_and_press_department_of_the_russian_mfa_on_the_introduction_of_eu_restric/

[150] owing link: https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-eu-european-union-response-to-promote-international-security-and-stability-in-cyberspace/ The Canadian and US endorsements can be found at the following links: https://www.state.gov/the-united-states-applauds-the-eus-action-on-cyber-sanctions/ y https://www.canada.ca/en/global-affairs/news/2020/07/canada-welcomes-european-unions-announcement-of-new-cyber-sanctions-listings.html

[151] See in this regard Resolution adopted by the UN General Assembly on 26 May 2021, A/RES/75/282 [without reference to a Main Committee (A/75/L.87/Rev.1 and A/75/L.87/Rev.1/Add.1)] according to which a draft is to be provided to the GA at its 78th session, which will begin in September 2023 and conclude in September 2024.

that "the EU does not see a need for any new legal instrument on cybercrime at UN level". [152] However, it appears that a few months later the EU shifted, as the May 2022 Cyber Posture seems to support the UN Convention as an effective instrument. In the terms used by the Cyber Posture: "the EU and its Member States will actively engage in the negotiations for a future UN Convention to serve as an effective instrument for law enforcement and judicial authorities in the global fight against cybercrime".[153]

88. The Strategy also proposed the development of "an informal EU Cyber Diplomacy Network "to promote the EU vision of cyberspace, exchange information and regularly coordinate on developments in cyberspace."[154] To this extent, the May 2022 Cyber Posture provided some more information about the envisaged EU Cyber Diplomacy Network by calling upon the High Representative "to establish the EU Cyber Diplomacy Network by Q3 2022, contributing to the exchange of information, joint training activities for EU and Member States' staff, coherent capacity building efforts and strengthening the implementation of the UN framework for responsible State behaviour as well as confidence-building measures between States."[155] This proposal has been welcomed by experts, notably in relation to the capacity for this Network to facilitate the setting up "meetings with stakeholders to identify potential collaboration in the joint training activities for EU and Member States' staff [as this] will allow both the EU and stakeholders to promote "targeted cooperation" in a much more effective way."

89. Finally, the Strategy also proposed the development of an EU External Cyber Capacity Building Agenda and an EU Cyber Capacity Building Board to support partners to increase their cyber resilience and capacities to investigate and prosecute cybercrime, mainly on the Western Balkans and in the EU's neighbourhood.[156] In this regard, the Strategic Compass went one step further in noting that "We will support our partners in enhancing their cyber resilience and, in cases of cyber crises, deploy EU and Member States' experts to offer support",[157] and the Cyber Posture confirmed that the EU Cyber Capacity Building Board is foreseen by the third quarter of 2022.[158]

90. In relation to the foregoing, the development of the EU Cyber Capacity Building Board has the potential to strengthen the EU's cyber capacity building efforts, notably by coordinating the significant number of initiatives and projects that the EU has undertaken in this area. Indeed, as several experts have recently underlined, there is a need to create more synergies across policy areas and communities, and to define objective criteria and identify priority areas for cyber capacity building project investments in order to avoid overlaps and duplicative efforts.[159]

V. Conclusions

91. In the light of the foregoing considerations, a number of conclusions can be highlighted.

[152] Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, cit., at p. 21.

[153] Council conclusions on the development of the European Union's cyber posture, Brussels, 23 May 2022, 9364/22, at p. 13.

[154] Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, cit., at p. 22.

[155] Council conclusions on the development of the European Union's cyber posture, Brussels, 23 May 2022, 9364/22, at p. 15.

[156] Id. pp. 22-23. See in this regard also A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security, cit., at p. 46: "we will in particular [...] Strengthen our security and defence cooperation with the Eastern partners with a view to strengthening their resilience, including against hybrid attacks and cyber threats, and boost tailored support and capacity building in the area of security and defence".

[157] A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security, cit.

[158] Council conclusions on the development of the European Union's cyber posture, Brussels, 23 May 2022, 9364/22, at p. 14.

[159] See in this regard R.J. ricart, D. van duren, and R. bosc, European Cyber Agora, Working Group 4: Advancing a global and open cyberspace Conclusions and recommendations, pp. 27-30.

92. First, the EU has been successful in obtaining international recognition as a relevant actor in the cybersecurity area. In particular, through bilateral and multilateral dialogues and cyber capacity building the EU has been able to influence other actors, for example in relation to the ratification of the Budapest Convention on cybercrime, and to be regarded as an interlocutor - a moderator - capable of contributing positively to cyberspace. Indeed, through the external dimension of cybersecurity, the EU has been able, it is submitted, to reinforce its role an international actor, and particularly as an international legal player.[160]

93. Second, the EU holds the potential to significantly contribute to (re)defining international norms and standards related to cybersecurity. In particular, the EU could contribute to the development of international law in the field of countermeasures, notably by defending the possibility of adopting voluntary collective countermeasures in some instances. In addition, the EU can also contribute to clarifying the cyber conduct that the EU and its Member States consider through the framework of restrictive measures in response to cyber-attacks and by shedding light on the grave instances under which a cyber-attack is liable to trigger the applicability of Article 42(7) in the EU context (and Article 51 of the UN Charter).

94. Third, the EU is particularly well-positioned to provide specific content to the due diligence principle in the cyberspace under international law by promoting externally the high cybersecurity and data protection standards that is adopting internally, and by raising awareness about the malicious cyber activities that are seemingly taking place in the territory of third countries through the adoption of restrictive measures. In addition, the EU could contribute to defending the mandatory character of the due diligence principle under international law in bilateral and multilateral, especially after the withdrawal of the United Kingdom from the EU, that contests such binding nature.

95. Finally, in order to be more influential in the international sphere, and be able to export its normative priorities as it has done in other areas,[161] it is submitted that the EU will need to show more unity and cohesion in international negotiations, but also internally, given the close interconnection of the internal and external dimensions of cybersecurity. A number of measures could be adopted in this regard, and some of them have already been suggested in official documents, such as the reinforcement of the joint intelligence gathering, or the adoption of a more effective and simplified decision-making, which could include the streamlining of QMV for the adoption of sanctions. Finally, the joint attribution of cyber-attacks to State actors at EU level could contribute to increase the purported deterrence effect of the EU restrictive measures and to bring the framework also more in line with international law.

[160] M. Cremona, 'Extending the Reach of EU Law: The EU as an International Legal Actor' in M. Cremona, /J. Scott (eds), *EU Law Beyond EU Borders The Extraterritorial Reach of EU Law*, cit. pp. 64-111. See also A. Bradford *The Brussels Effect How the European Union Rules the World* (OUP 2020).

[161] G. Monti, 'The Global Reach of EU Competition Law' in m. cremona, and j. scott (eds), *EU Law Beyond EU Borders The Extraterritorial Reach of EU Law*, cit. p. 193.