

ARTICLE

Special Issue: International Law and Digitalization

# The Rationale and the Perils of Failing to Invoke State Responsibility for Cyber-Attacks: The Case of the EU Cyber Sanctions

Sara Poli<sup>1</sup>  and Emanuele Sommario<sup>2</sup>

<sup>1</sup>University of Pisa, Pisa, Italy and <sup>2</sup>Sant'Anna School of Advanced Studies, Pisa, Italy

**Corresponding author:** Sara Poli; Email: sara.poli@unipi.it

(Received 10 April 2023; accepted 10 April 2023)

## Abstract

Malicious cyber activities are on the rise. States and other relevant actors need to constantly adapt to the evolving cyber threat landscape, including by setting up effective deterrence mechanisms. This is what the European Union (EU) has done through the adoption of Common Foreign and Security Policy (CFSP) Decision 2019/797, which allows it to impose targeted sanctions to deter and respond to cyberattacks that constitute an external threat to the EU or its member states. However, in contrast to other horizontal regimes of restrictive measures in force within the EU, foreign governments are not included as potential targets of cyber sanctions. Moreover, the recital of the Decision specifies that the adoption of restrictive measures does not involve attribution of international responsibility for cyber-attacks to a third State. This article aims at identifying the rationale behind the inclusion of these distinctive features. It starts by considering the legal uncertainty that surrounds attribution of international responsibility for cyber operations. Next, it explains why the EU is not well placed to invoke third-State responsibility, and the reasons behind its reluctance to do so. It will then illustrate the risks inherent in the lack of a clear legal framework to attribute the responsibility of cyber-attacks to third countries. This may have serious consequences in terms of legal certainty when a cyber-attack amounts to a breach of the prohibition on the use of force in international relations. Then, we explore recent developments in EU legislation in the area of cyber security and the possibility to strengthen the powers of the European Union Agency for Cybersecurity (ENISA). We draw two conclusions: first, the Union might develop the capacity to attribute cyber attacks to specific actors and there is an interest to do so. However, Member States are probably still reticent to take this step. Two, despite the advantages of establishing a reliable attribution mechanisms, it is submitted that the majority of States prefers to take advantage of a regulative gap that allows them to react to cyber incidents as they see fit.

**Keywords:** Cyber-attack; attribution of conduct; state responsibility; cyber restrictive measures; EU Common Foreign and security Policy; European Union Agency for Cybersecurity (ENISA)

## A. Introduction

Human activity in the cyberspace may pose significant problems to the international community. States and societies have grown highly dependent on the functioning of information technology (IT) infrastructure and this, in turn, has generated new digital vulnerabilities. Indeed, only limited resources are needed to cause significant harm, capable of jeopardizing international stability.<sup>1</sup> Although cyberspace provides many business opportunities for individuals and is vehicle for the right of expression, it may be used for criminal and politically motivated cyber-attacks, including state-sponsored ones. These events may prompt reactions both by governments and international organizations. In the context of the European Union (EU)<sup>2</sup> the Council has—independently of the United Nations (UN)—adopted unfriendly measures as a reaction to these attacks. Common Foreign and Security Policy (CFSP) Decision 2019/797<sup>3</sup> imposes restrictive measures against cyber-attacks with a potentially significant effect “which constitute an external threat to the Union or its Member States.”<sup>4</sup> These attacks must be carried out from outside the Union in order to fall within the scope of the Union’s restrictive measures.<sup>5</sup> The sanctions might also apply in case the targets of these attacks are third States or international organizations.<sup>6</sup>

In this essay, we focus on the legal problems connected to “cyber-attacks” because they present special features with respect to other forms of malicious cyber activities.<sup>7</sup> While a universally agreed definition<sup>8</sup> is not available, in the Decision under exam, cyber-attacks are described as “[a]ctions involving any of the following: (a) access to information systems; (b) information system interference; (c) data interference; or (d) data interception, where such actions are not duly authorised by the owner or by another right holder of the system or data or part of it, or are not permitted under the law of the Union or of the Member State concerned.”<sup>9</sup> Article 1(4) of the mentioned Decision contains a non-exhaustive list of these targets which include: “(a) critical infrastructure, such as submarine cables and objects launched into outer space, which is essential for the maintenance of vital functions of society, or the health, safety, security, and economic or social well-being of people; b) services necessary for the maintenance of essential social and/or economic activities, in particular in the sectors of: energy (electricity, oil and gas); transport (air, rail, water and road); banking; financial market infrastructures; health (healthcare providers, hospitals and private clinics); drinking water supply and distribution; digital infrastructure; and any other sector which is essential to the Member State concerned; (c) critical State functions, in

<sup>1</sup>See *On the Application of International Law in Cyberspace*, THE GERMAN FEDERAL GOVERNMENT, 1 (Mar. 2021), <https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf>.

<sup>2</sup>See *Significant Cyber Incidents Since 2006*, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES, [https://csis-website-prod.s3.amazonaws.com/s3fs-public/220104\\_Significant\\_Cyber\\_Events.pdf?dLSQUtb9qiFpttFl7FcBmA9IKZaNPUib](https://csis-website-prod.s3.amazonaws.com/s3fs-public/220104_Significant_Cyber_Events.pdf?dLSQUtb9qiFpttFl7FcBmA9IKZaNPUib) (Updated list of cyber incidents against States and IOs occurring since 2003). The EU itself has been the direct victim of at least several cyber-attacks over the last few years.

<sup>3</sup>See Council Decision (CFSP) No. 2019/797 of 17 May 2019, 2019 O.J. (L 129 I/13) (concerning restrictive measures against cyber-attacks threatening the Union or its Member States).

<sup>4</sup>See *id.* at art. 1(1).

<sup>5</sup>See *id.* at art. 1(2) (“In order to qualify as a cyber-attack constituting an external threat, these attacks may (a) originate, or be carried out, from outside the Union; (b) use infrastructure outside the Union; (c) be carried out by any natural or legal person, entity or body established or operating outside the Union; or (d) be carried out with the support, at the direction or under the control of any natural or legal person, entity or body operating outside the Union”).

<sup>6</sup>See *id.*, art. 1(5).

<sup>7</sup>See *infra*, Section B.

<sup>8</sup>See G.A. Res. 74/247 (Jan. 20, 2020). Efforts to reach an agreement in the United Nations context have so far failed. As a result, the EU definition of cyber-attacks is different (and narrower) than that included in legislation in the United States. Indeed, the latter also cover cyber-enabled activities having the effects of “causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain”; See also Exec. Order No. 13,694 31 C.F.R. § 578 (2015). In contrast, this category of attack is not included in the Council Regulation under exam.

<sup>9</sup>See Council Decision (CFSP) 2019/797, *supra* note 3, at art. 1(3).

particular in the areas of defense, governance and the functioning of institutions, including for public elections or the voting process, the functioning of economic and civil infrastructure, internal security, and external relations, including through diplomatic missions; (d) the storage or processing of classified information; or (e) government emergency response teams.”<sup>10</sup> Thus, cyber-attacks are likely to have disruptive effects by virtue of the special importance of the targets (critical infrastructure) or of the essential nature of the functions or of the services that these targets perform.

EU cyber-sanctions can be adopted against natural persons, entities or bodies who are responsible for cyber-attacks or attempt to carry out such an attack<sup>11</sup> and may take the form of asset freezes and visa bans. These measures were adopted to respond and to deter cyber-attacks<sup>12</sup> and they are deprived of punitive purpose.<sup>13</sup> Cyber-sanctions can be seen as a complement to existing internal measures that approximate the criminal law of Member States applicable to cybercrime.<sup>14</sup> The aim of both instruments is to prevent potential authors of cybercrime or attacks from launching new ones.

The Union is a subject of international law autonomous from its constituent members and has competence to protect its security, including by adopting sanctions in reaction to cyber-attacks.<sup>15</sup> It is noteworthy that this is not an exclusive competence of the organization; therefore, Member States are also entitled to react to cyber-attacks on their own. However, while “national security remains the sole responsibility of each Member State,”<sup>16</sup> where the authors of a cyber-attack are natural persons, it is more effective for EU members to act through the Union<sup>17</sup> because the targeted individuals will be subject to an EU-wide asset freeze (and/or visa bans).

Two aspects of the sanction regime are particularly noteworthy. First, state organs or governments are not included in scope *ratione personae* of the cyber sanctions, in contrast to other horizontal regimes of restrictive measures in force within the EU such as those aimed at contrasting the use of chemical weapons or at preventing human rights abuses.<sup>18</sup> Second, Recital n. 9 of the Decision imposing sanctions for cyber-attacks states, “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

<sup>10</sup>*Id.* at art. 1(4).

<sup>11</sup>*See id.* at arts. 4–5.

<sup>12</sup>*See European Council Conclusions of 18 October 2018*, EUROPEAN COUNCIL (Oct. 18, 2018), <https://www.consilium.europa.eu/en/press/press-releases/2018/10/18/20181018-european-council-conclusions/>.

<sup>13</sup>*See generally* Council Decision (CFSP) No. 2020/1537 of 22 October 2020 *amending* Council Decision (CFSP) No. 2019/797 (The deterrent objective of cyber sanctions is confirmed by the motivation of single CFSP Decisions enacted to respond to specific cyber-attacks). Restrictive measures do not have a punitive purpose in the Council’s practice. *See also Sanctions Guidelines*, COUNCIL OF THE EUROPEAN UNION, 46 (May 4, 2018), <https://data.consilium.europa.eu/doc/document/ST-5664-2018-INIT/en/pdf>.

<sup>14</sup>The EU has adopted internal legislation seeking to approximate the criminal law of the Member States in the area of attacks to information systems. *See* Council Directive 2013/40, 2013 O.J. (L 218). This legislation builds upon the Convention on Cybercrime, Nov. 23, 2001, E.T.S. 185 (the so-called “Budapest Convention”). The EU has encouraged Member States to ratify this Convention. The purpose of this Treaty is, amongst others, to criminalise a number of activities against an information system. The Directive seeks to minimally harmonise criminal law concerning the definition of criminal offences and sanctions in the area of attacks of this kind.

<sup>15</sup>Indeed, the Union has the aim to safeguard its security. *See* The Treaty of European Union art. 21 (3)(a). *See infra* note 17.

<sup>16</sup>*See id.* at art. 4(2). This makes it possible for Member States to react to cyber-attacks independently of the EU.

<sup>17</sup>*See id.* at art. 29. This is the legal basis of CFSP Decisions instituting restrictive measures. In case an act is deemed necessary for the purpose of applying the CFSP Decision, a Regulation is adopted, under The Treaty on the Functioning of the European Union art. 215, to introduce financial restrictive measures [hereinafter “TFEU”].

<sup>18</sup>With respect to sanctions directed at contrasting the proliferation and use of chemical weapons, *see* Council Decision (CFSP) No. 2018/1544 of 15 October 2018, art. 2(1). On restrictive measures aimed at addressing serious human rights violations and abuses, *see* Council Decision (CFSP) No. 2020/1999 of 7 December 2020, art. 2(1).

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.”<sup>19</sup>

In this Article, we aim to explore the rationale behind the inclusion of the mentioned Recital; in particular we are interested in understanding whether the nature of cyber activities is such as to require a distinctive treatment with respect to that reserved to other “non-cyber” threats to peace and security. In order to provide an answer we will examine the text of the instituting Decision of cyber sanctions and the way the latter was applied in the practice. The article will first look at the reasons which make the attribution of cyber-attacks a difficult endeavor, thus contributing to a lack of legal clarity (section B). Then, we bring the reader’s attention to the EU’s reluctance to invoke state responsibility and we identify the possible reasons behind this choice (Section C). Next, we examine the inherent risks of failing to develop a solid legal framework in relation to cyber-threats and the underlying motivations (Section D). Then, we show that the trend of expanding the EU legislation in the area of cyber activities has not ceased since 2008 when internal legislation seeking to harmonize security requirements at national level was enacted so as to be able to better address cyber-attacks or malicious activities (section E); we also consider that the EU has an interest and potential capacity to develop an attribution mechanism for cyber-attacks. Yet, we conclude that although the creation of an autonomous capacity in the EU to attribute cyber-attacks would present certain advantages for some Member States, it is not clear whether it would be possible for the EU organs to develop an attribution mechanism due to the uncertain boundaries of EU’s competence (Section E). We finally suggest that, even beyond the EU, a possible way forward would be to agree on a multilateral attribution mechanism. Yet, at the moment, there is no sufficient interest in the international community for such an initiative (Section F).

## B. Difficulties in Establishing State Responsibility for Cyber-Attacks

While the application of international law to cyberspace was the object of some controversies in the past,<sup>20</sup> it is now undisputed that the principles of sovereignty, non-intervention, the prohibition on the use of force and other general rules of international law apply to states’ cyber activities as they do in the analogical world.<sup>21</sup> Yet, it is still far from clear how traditional principles of international law need to be transposed in the cyber domain.<sup>22</sup> In truth, there seems to be a general trend among States to refrain from establishing rigid legal frameworks in the area of cyber operations, also in light of the fast technological development.<sup>23</sup> Many States have chosen to adopt a policy of silence and ambiguity about how international law applies in cyberspace.<sup>24</sup> As stated by former US Department of State Legal Advisor Brian Egan, the international community is

<sup>19</sup>See Council Decision (CFSP) No. 2019/797, *supra* note 3, at recital n. 9.

<sup>20</sup>See David R. Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

<sup>21</sup>Within the UN, the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) has held a number of meetings since 2004 to discuss the application of international law to cyber activities. In its 2013 Report to the UN General Assembly, it stated unequivocally that “State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.” See Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 20, U.N. Doc. A/68/98 (Jun. 24, 2013).

<sup>22</sup>See Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention*, CHATHAM HOUSE (Dec. 2, 2019), <https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks>.

<sup>23</sup>See Iryna Bogdanova & Maria Vasquez Callo-Müller, *Unilateral Cyber Sanctions: Between Questioned Legality and Normative Value*, 54 VAND. J. TRANSNAT’L L. 915 (2021).

<sup>24</sup>See Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 AM. J. INT’L L. 583 (2018).

currently faced “with a relative vacuum of public State practice.”<sup>25</sup> This uncertainty pertains both to the very qualification of malicious cyber operations as breaches of international law (i.e. to whether any primary norm is actually breached), but also to the difficult exercise of attributing cyber-attacks to a specific State actor (i.e. whether the conduct can be imputed to a specific subject of international law).<sup>26</sup>

Starting with the first issue, not all malicious cyber activities – including those defined as cyber-attacks under Decision 2019/797 – constitute breaches of international law. There are different categories of cyber activities that could be defined as “malicious”, including cyber crime or cyber espionage. Cyber-crime, for instance, does not call necessarily into question the international responsibility of States because it is a form of crime that may be carried out by non-state entities. The most important multilateral Treaty in this area is the Council of Europe “Budapest Convention” of 2001,<sup>27</sup> which has 66 Parties, including 26 EU Member States.<sup>28</sup> This Treaty imposes on its Parties obligations to criminalize a wide range of conducts.<sup>29</sup>

Cyber espionage, however, involves cyber activities that are carried out with the objective of obtaining information. It is a form of cyber-crime because it amounts to an illegal access to a computer system. Some of the activities against which the EU has imposed restrictive measures might fall under this category. The Tallin Manual 2.0 defines cyber espionage as “an act undertaken clandestinely or under false pretences that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party.”<sup>30</sup> However, many experts contend that there is no prohibition in international law on espionage per se,<sup>31</sup> and on cyber espionage in particular. The experts working on the Tallin Manual 2.0, for instance, could not reach a consensus as to whether remote cyber espionage violated international law. While the majority believed that the exfiltration of data violated no rule of international law, a few believed that at some point the data breach might be so severe as to make it illegal.<sup>32</sup> Similarly, the experts did not agree on the legality of close-access operations, such as operations where an individual in the territory of the target state inserts a USB drive into a government

<sup>25</sup>See Brian Egan, Legal Advisor to the Dep’t of State, Remarks on International Law and Stability in Cyberspace at the University of California, Berkeley, School of Law, JUST SECURITY (Nov. 10, 2016), <https://www.justsecurity.org/wp-content/uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf>.

<sup>26</sup>This bipartition reflects the element for an internationally wrongful act identified in the Articles on State Responsibility developed by the International Law Commission. See Draft Articles on Responsibility of States for Internationally Wrongful Acts, Rep. of the Int’l Law Comm’n on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10 (2001) art. 2 [hereinafter “ARSIWA”]. The same principles apply if the responsibility of an IO is at stake, see Rep. of the Comm’n to the G.A. on the Work of its Sixty-Third Session, 2 Y.B. Int’l L/ Comm’n, U.N. Doc. A/66/10 (2011).

<sup>27</sup>See comments, *supra* note 13.

<sup>28</sup>See Proposal for a Council Decision Authorising Member States to Ratify, in the Interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, COM (2021) 719 final (Nov. 25, 2021), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0719>. The European Commission has urged Member States to ratify this Treaty since this Treaty is open to third countries but not to international organizations. As of August 2022, all Member States, except Ireland, have ratified this Convention; all of them were recently invited by the Commission to ratify the second additional protocol designed to enhance cooperation on cybercrime and the collection of evidence in electronic form of a criminal offence for the purpose of specific criminal investigations or proceedings.

<sup>29</sup>These include: illegal access to the whole or any part of a computer system without right, illegal interception of non-public transmissions of computer data to, from or within a computer system, the damaging, deletion, deterioration, alteration or suppression of computer data, system interference and misuse of devices, computer related forgery and fraud, conducts related to pornography and infringements of copyright and related rights. Council Directive 2013/40, *supra* note 14, imposes a requirement on Member States to criminalize some of the attacks to information systems mentioned above.

<sup>30</sup>See MICHAEL N. SCHMITT, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 410 (2d. ed. 2017). The Tallinn Manual is one of the most important contemporary documents regarding the application of international law to cyberspace. However, according to important authors, an analysis of state practice reveals that the rules set out in the Manual do not all enjoy general acceptance by states. See Efrony & Shany, *supra* note 24, at 585.

<sup>31</sup>See A. John Radsan, *The Unresolved Equation of Espionage and International Law*, 28 MICHIGAN J. INT’L L. 595 (2007).

<sup>32</sup>See SCHMITT, *supra* note 30, at 170–171.

system to steal or alter data. Clearly, there is a lack of a shared understanding among States on what is allowed and what is proscribed in the cyber domain. This makes the determination of an objective breach of international law a rather complex task.

Turning now to the issue of attribution, one of the biggest challenges for a State that finds itself a victim of a hostile cyber operation is ascertaining who was behind it. Even if a certain cyber-attack is considered to represent a breach of state sovereignty, without clearly identifying who is responsible for the hostile cyber activity it is difficult to take any targeted action in response. The problem of attribution in the context of cyber activities has generated a great deal of discussion among scholars.<sup>33</sup> The Tallin Manual 2.0 addresses the issue by echoing Articles 4 and 5 of the Articles of State Responsibility,<sup>34</sup> accordingly to which cyber operations conducted by state organs are generally attributable to the state. Even though this approach reflects international law in non-cyber situations, its application to cyber activities is not without controversy. For example, the experts noted that traditionally the use of government assets such as tanks or warships was a near irrefutable indication that such activity should be attributed to a that state. The same cannot be said of cyber activities. Indeed, given the ability to capture or spoof cyber infrastructure, including where the cyber activities might originate from, “the mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure, or that malware used against hacked cyber infrastructure is designed to “report back” to another State’s governmental cyber infrastructure, is usually insufficient evidence for attributing the operation to that State.”<sup>35</sup> Moreover, even if the actual material source of a specific cyber activity has been ascertained, “identifying the persons, organizations, or states that are legally responsible for the cyber-attack remains challenging.”<sup>36</sup> As some scholars claim, “although legal attribution relies on forensic evidence produced by technical attribution in order to make determinations and justify legal action in the form of indictments, sanctions or countermeasures, forensic evidence needs to be interpreted and assessed according to legal criteria.”<sup>37</sup> In other words, the technical attribution is a precondition for the legal attribution to an individual state organ but is not sufficient in itself to legally ascribe the conduct to a given State.

The challenge, however, is not simply with the law. As with other forms of hostile activity, there are technical, political and diplomatic considerations in publicly attributing hostile cyber activity to a State, in addition to whether the legal test is met. Such political considerations concern the question of whether to attribute and when; whether attribution will be public or private; and what will be attributed and to whom.<sup>38</sup> This predominantly political process may lead to action “such as diplomatic demarches, public denunciations or restrictive measures,”<sup>39</sup> but leaves open the question of the exact legal responsibility originating from the cyber-attack. As will be shown, the complexity of the legal and political issues involved has even more important ramifications when an attribution process needs to be conducted within a supranational organization such as the EU.

<sup>33</sup>See *AJIL Symposium on Cyber Attribution*, AM. J. INT’L L., <https://www.cambridge.org/core/journals/american-journal-of-international-law/ajil-unbound-by-symposium/cyber-attribution>. See also Nicholas Tsagourias, *Cyber-attacks, Self-Defence and the Problem of Attribution*, 17 J. CONFLICT & SEC. L. 229 (2012).

<sup>34</sup>See SCHMITT, *supra* note 30, at 87–90.

<sup>35</sup>See *id.* at 91. See also Rep. of the G.A., at 10, U.N. Doc. A/76/135, (2021) (stating that “[a]n ICT incident emanating from the territory or the infrastructure of a third State does not, of itself, imply responsibility of that State for the incident”).

<sup>36</sup>See William Banks, *The Bumpy Road to a Meaningful International Law of Cyber Attribution*, 113 AM. J. INT’L L. 191 (2019).

<sup>37</sup>See Nicholas Tsagourias & Michael Farrell, *Cyber Attribution: Technical and Legal Approaches and Challenges*, 31 EUR. J. INT’L L. 943 (2020).

<sup>38</sup>According to the UK Advocate-General: “[T]he UK can and does attribute malicious cyber activity where we believe it is in our best interests to do so, and in furtherance of our commitment to clarity and stability in cyberspace. Sometimes we do this publicly, and sometimes we do so only to the country concerned. We consider each case on its merits.” See Jeremy Wright, *Cyber and International Law in the 21st Century*, GOV.UK (May 23, 2018), <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>.

<sup>39</sup>See Tsagourias & Farrell, *supra* note 37, at 943.

### C. The EU's Reluctance to Rely on State Responsibility in the Context of the Cyber Restrictive Measures

It is submitted that the existence of evidentiary and legal hurdles in the process of attribution contributes to explain the absence of an explicit reference to third countries in the list of addresses of cyber sanctions as well as the clause in Recital n. 9. The EU is free to target the authors of the attack (natural persons or other non-state entities) on the basis of the technical attribution.<sup>40</sup> In contrast, the right to trigger the rules on the responsibility of the State is reserved to individual Member States. The implicit reference is to the State(s) whose territory/ies has or have been affected by a cyber-attack. In some cases EU members have the capacity to attribute a cyber-attack to a certain third country. Yet, not all EU Members may have the necessary capability to do so.<sup>41</sup> In case one EU member is not affected by the cyber-attack and does not have the capacity to verify the forensic evidence provided by the State target of the attack, it may refrain from triggering state responsibility.<sup>42</sup> This is because there may be a lack of trust between the European national authorities if only some of them have the capacity to identify the authors of a cyber-attack. Probably, it is because of this situation and of intelligence activities gaps that the EU Council opted to specify that the EU does not attribute the cyber activity to a state and left the decision to trigger state responsibility to each Member state. In the Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (Cyber Diplomacy Toolbox) the Council remarks: "The EU reminds that attribution to a State or a non-State actor remains a sovereign political decision based on all-source intelligence and should be established in accordance with international law of State responsibility. In that regard, the EU stresses that not all measures of a joint EU diplomatic response to malicious cyber activities require attribution to a State or a non-State actor."<sup>43</sup> At the same time, the Commission and the High Representative of the Union for foreign affairs and security policy have stressed that currently there is limited mutual cooperation between Member States and no operational mechanism between the latter and EU institutions, agencies and bodies is in place, in the event of a large-scale, cross-border cyber incidents or crisis.<sup>44</sup>

In sum, it seems that the reasons why the clause is included in Recital n. 9 is that the EU, as a subject of international law, intended to refrain from invoking state responsibility. Member States's representatives in the Council probably preferred to reserve this decision for themselves. As mentioned in Section A, in principle, Member States have the primary responsibility to protect their internal security and they may react to cyber-attacks on their own.

Another possible reason explaining the EU's decision to leave to Member States the choice to invoke state responsibility is that the organization has started to exercise its competence in the area of cyber activities quite recently. The first Directive in the field of cybersecurity was enacted

<sup>40</sup>This process may take some time. It is not coincidental that there was a delay of several months in the adoption of the EU restrictive measures after the cyber-attack which hit Germany and the Organization for the Prohibitions of Chemical Weapons (OPCW).

<sup>41</sup>Only Sweden, the Netherlands, Estonia, Austria, France and Germany have these attribution capabilities and the political will to share information with other Member States. See Annegret Bendiek & Matthias Schuleze, *Attribution: A Major Challenge for EU Cyber Sanctions*, STIFTUNG WISSENSCHAFT UND POLITIK (Dec. 2021), [https://www.swp-berlin.org/publications/products/research\\_papers/2021RP11\\_EU\\_CyberSanctions.pdf](https://www.swp-berlin.org/publications/products/research_papers/2021RP11_EU_CyberSanctions.pdf).

<sup>42</sup>On the politics of attribution, see *id.* at 10–14.

<sup>43</sup>See *Outcome of Proceedings*, COUNCIL OF THE EU (Jun. 19, 2017), <https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf>. That "Attribution is a sovereign political decision by a State" is also underlined in an unofficial document of the Enisa. See also *Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities "Cyber Diplomacy Toolbox"*, EUROPEAN UNION EXTERNAL ACTION, <https://www.enisa.europa.eu/events/artificial-intelligence-an-opportunity-for-the-eu-cyber-crisis-management/workshop-presentations/20190603-eeas-eu-cyber-diplomacy-toolbox.pdf>.

<sup>44</sup>See *Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade*, EUR-LEX (2020), <https://eur-lex.europa.eu/legal-content/ga/TXT/?uri=CELEX:52020JC0018>.

in 2008<sup>45</sup> on the basis of the “implicit powers” provisions (the then Article 308 of the Treaty on the European Community) and its scope was limited.<sup>46</sup>

At the moment, there are no harmonized evidentiary standards on how to identify authors of cyber-attacks which could be taken into account by national authorities. Therefore, in case these events occur the EU has self-imposed a restriction on engaging state responsibility of the third State in which the authors of the attack operated and has also limited the range of possible measures that can be taken when those actors carry out a cyber-attack. The EU has confined itself to make it possible for the Council to freeze the assets of (or to impose admission restrictions on) natural or legal persons and has listed individual state organs,<sup>47</sup> relying on the intelligence provided by the Member States,<sup>48</sup> without triggering state responsibility.

Turning to the practice, the EU has made a modest use of cyber-sanctions. So far, these measures were imposed in response to only three distinct episodes: the first one concerned a single Member State while the second one affected a group of them; the third one was an attempted cyber-attack directed against an international organization located in one EU Member State. As mentioned above, the target of the first attack was the German Bundestag in 2015.<sup>49</sup> Being a state organ, this is a sensitive target. MPs received bogus emails containing a link that led to the installation of malware on their computers. The malware was able to spread and eventually infiltrated the networks of the Parliament and allowed hackers to access internal confidential communication data, schedules, and other sensitive data.<sup>50</sup> The attack was linked to the hacker group APT28, an actor believed to be associated with the Russian military intelligence.<sup>51</sup> The second attack (2016-2017) was dubbed “Operation Cloud Hopper” and was directed at managed service providers located in at least fifteen States, including five EU Member States.<sup>52</sup> The hackers installed malware and hacking tools to access systems and steal data,<sup>53</sup> causing significant economic loss. The operation was conducted by cyberespionage group APT10 which is allegedly sponsored by the Chinese government.<sup>54</sup> The last attack was an attempt by Russian intelligence agents to infiltrate the Wi-Fi network of the Organisation for the Prohibition of Chemical Weapons (OPCW) in The Hague.<sup>55</sup> While conducting the operation, the attackers had been observed and were subsequently arrested by the Dutch military intelligence and no concrete damage was caused. The arrest facilitated the attribution process as all four operatives were clearly

<sup>45</sup>See Council Directive 2008/114/EC, 2008 O.J. (L 345). This is also known as the “European Critical Infrastructure” (ECI) Directive. See *infra*, Section F.

<sup>46</sup>See Johan David Michels & Ian Walden, *Beyond “Complacency and Panic:” Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure?*, 45 EUR. L. REV. 25 (2020). This directive only addressed the energy and transport sectors.

<sup>47</sup>For example, this has happened with respect of Russian members of the military forces for a cyber-attack to the German Bundestag.

<sup>48</sup>To our knowledge, Germany also refrained from attributing the malicious conduct to Russia.

<sup>49</sup>See Council Decision (CFSP) No. 2020/1537, *supra* note 13.

<sup>50</sup>See Von Maik Baumgärtner et al., *Cyberangriff auf den Bundestag*, SPIEGEL NETZWELT (May 15, 2015), <https://www.spiegel.de/netzwelt/netzpolitik/cyber-angriff-auf-den-deutschen-bundestag-a-1033984.html>.

<sup>51</sup>See Russia “Was Behind German Parliament Hack”, BBC NEWS (May 13, 2016), <https://www.bbc.com/news/technology-36284447>.

<sup>52</sup>See *Operation Cloud Hopper: What You Need to Know*, TREND MICRO (Apr. 10, 2017), <https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/operation-cloud-hopper-what-you-need-to-know>. See also Council Decision (CFSP) 2020/1748 of 20 November 2020 amending Council Decision (CFSP) 2019/797, O.J. 2020 (L 393).

<sup>53</sup>See *Operation Cloudhopper* (2017), CCCDCOE (2017), CYBERLAW, [https://cyberlaw.ccdcoe.org/wiki/Operation\\_Cloudhopper\\_\(2017\)](https://cyberlaw.ccdcoe.org/wiki/Operation_Cloudhopper_(2017)).

<sup>54</sup>See Lucian Constantin, ‘Five Eyes’ Countries Attribute APT10 Attacks to Chinese Intelligence Service, SECURITY BOULEVARD (Dec. 21, 2018), <https://securityboulevard.com/2018/12/five-eyes-countries-attribute-apt10-attacks-to-chinese-intelligence-service>.

<sup>55</sup>See *How the Dutch Foiled Russian “Cyber-attack” on OPCW*, BBC NEWS, (Oct. 4, 2018), <https://www.bbc.com/news/world-europe-45747472>. See also Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797, O.J. 2020 (L 246).

linked to the Russian military intelligence service. Five states (Australia, Canada, the Netherlands, New Zealand and the United Kingdom) coordinated accusations that the latter was responsible for a series of cyber operations including the one at the OPCW.<sup>56</sup> Notwithstanding the involvement of Russian and Chinese State agents, the EU refrained from attributing legal responsibility to either of the sending States, thereby restating its unwillingness to engage in this exercise.

#### D. The Perils of the Reluctance to Agree Common Standards on the Attribution of Responsibility to a State for Carrying out Cyber-Attacks

Clearly the current state of affairs with respect to the rules on the attribution of responsibility for malicious cyber activities is not satisfactory. The lack of a more settled legal framework potentially entails huge economic costs.<sup>57</sup> But the possible damage is not only of economic or financial nature. The reputational harm caused by cyber-interferences with electoral processes, for instance, is difficult to quantify but has the potential to undermine the political stability of entire countries.<sup>58</sup> Even more worrying is the prospect that a cyber-attack crosses the threshold required to be considered a “use of force” under Article 2(4) of the UN Charter and trigger the right to individual or collective self-defense foreseen by the Charter and customary international law.<sup>59</sup>

While the practice of States and international organizations is only beginning to clarify how cyber operations must be addressed under the *jus ad bellum*,<sup>60</sup> there is widespread consensus among States and scholars that a cyber-attack can amount to a violation of the prohibition of the use of force. As is known, the International Court of Justice (ICJ) has stated that Articles 2(4) and 51 of the UN Charter, apply to “any use of force, regardless of the weapons employed.”<sup>61</sup> Thus, if a computer network is used instead of a traditional kinetic weapon this will not prevent the classification of the cyber operation as a “use of force.” According to the majority view, the decisive factor to distinguish a cyber operation that qualifies as “use of force” from less serious breaches is the scale and severity of its consequences.<sup>62</sup> This stance is reflected in the Tallin Manual 2.0, according to which “[a] cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.”<sup>63</sup> It is beyond the scope of the present Article to examine the different factors that might influence the assessment at hand; yet, it is worth emphasizing that attacks on critical infrastructure – such as the ones listed in Decision (CFSP) 2019/797 – have a higher probability of reaching the “use of force” threshold.<sup>64</sup> The idea that cyber-operations may breach the prohibition on the use of force

<sup>56</sup>See Martha Finnemore & Duncan B. Hollis, *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity*, 31 EUR. J. INT’L L. 969, 972 (2020).

<sup>57</sup>Losses related to cybercrime have reached staggering dimensions in 2021 with damages amounting to six trillion USD, and with estimations that this sum will almost double by 2025. See Steve Morgan, *Cybercrime To Cost The World \$10.5 Trillion Annually By 2025*, CYBERCRIME MAGAZINE (Nov. 13, 2020), <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>.

<sup>58</sup>See Myriam Dunn Cavelty & Andreas Wenger, *Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science*, 41 CONTEMP. SEC. POL’Y 5 (2020).

<sup>59</sup>For an accurate analysis of the issue, see MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 43–116 (2014).

<sup>60</sup>This expression refers to the branch of international law regulating the legitimacy of the use of force in international relations. See Reese Nguyen, *Navigating Jus Ad Bellum in the Age of Cyber Warfare*, 101 CALIF. L. REV. 1079 (2013).

<sup>61</sup>See *Military and Paramilitary Activities In and Against Nicaragua* (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶¶ 188–190 (June 27). See also *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 1986 I.C.J. ¶ 39 (Jul. 8).

<sup>62</sup>Other theories put forward by scholars include the “instrument-based” approach, which gives weight to the form of weapon used to perpetrate an attack, and the “target-based” approach, which automatically treats any cyberattack against critical national infrastructure as an armed attack because of the potential for severe consequences if such systems are disabled. For a critique on these two approaches, see Nguyen, *supra* note 60, at 1117–21.

<sup>63</sup>See SCHMITT, *supra* note 30, at 330.

<sup>64</sup>*Id.* at 337.

and that the consequences of the attack are decisive in this assessment is also supported by the national positions of several States, including Australia,<sup>65</sup> Germany,<sup>66</sup> Italy,<sup>67</sup> and the US.<sup>68</sup> Moreover, particularly severe cases of “use of force” may qualify as “armed attacks” and therefore entitle the victim State to lawfully use force in self-defense.<sup>69</sup> The type of force employed by the injured state is not necessarily limited to taking measures by cyber means as it can make resort to kinetic means, as long as the response is necessary, proportionate and in accordance with other provisions of international law.<sup>70</sup>

The lack of commonly agreed standards on the attribution of responsibility to a State for carrying out cyber-attacks bears important risks. There seems to be agreement that a State may use kinetic force in response to a cyber-attack that meets the definition of “armed attack” under the *jus ad bellum*, and yet the uncertainty that surrounds the issue of attribution opens the way to dangerous mistakes. Brazil’s position paper on the application of international law to cyberspace underlines that “technical, legal and operational challenges to determine attribution might make it impossible to verify potential abuses of the right of self-defense, which in turns creates the risk of low impact persistent unilateral military action undermining the collective system established under the Charter.”<sup>71</sup> In the absence of any reliable verification mechanism, when a cyber-attack amounts to a “use of force” or to an “armed attack,” the target State will find itself in a problematic condition of uncertainty. Ultimately, the state (or the International Organization) concerned will either not be able to protect its security or risk to use force against a State without being certain that it was at the origin of the cyber-attack. A real need for a clearer legal framework exists, as the current lack of certainty might lead to arbitrary unilateral reactions. As Wright notes, “if we accept that the challenges posed by cyber technology are too great for the existing framework of international law to bear, that cyberspace will always be a grey area, a place of blurred boundaries, then we should expect cyberspace to continue to become a more dangerous place.”<sup>72</sup>

Considering the challenges highlighted above and the specific rules laid down in Recital n. 9 of the EU Decision on cyber sanctions, it is necessary to examine whether there is a special attention within the EU towards the setting up of a verification mechanism. In principle the EU should be particularly sensitive to this problem because it shares with its Member States the competence to address cyber-attacks and in case of an armed attack there is a special mutual defense clause in the EU Treaty<sup>73</sup> requiring Member States to assist the victim of the attack. It is therefore interesting to review the terms of the discussion on the setting up of a verification mechanism in this context.

<sup>65</sup>See Annex B: Australia's Position on How International Law Applies to State Conduct in Cyberspace, AUSTRAL. GOV'T, <https://www.internationalcybertech.gov.au/our-work/annexes/annex-b>.

<sup>66</sup>See *On the Application of International Law in Cyberspace*, *supra* note 1, at 5.

<sup>67</sup>See Italian Position Paper on “International law and Cyberspace,” ITALIAN MINISTRY FOR FOREIGN AFFS. AND INT’L COOP., [https://www.esteri.it/mae/resource/doc/2021/11/italian\\_position\\_paper\\_on\\_international\\_law\\_and\\_cyberspace.pdf](https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf).

<sup>68</sup>See DOD General Counsel Remarks at U.S. Cyber Command Legal Conference, U.S. DEP’T OF DEF. (Mar. 2, 2020), <https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/>.

<sup>69</sup>As is known, Art. 51 of the UN Charter reaffirms the right to self-defense “if an armed attack occurs” against a Member State. In the Nicaragua Judgment, *supra* note 61, the ICJ distinguished the “most grave” form of “use of force” from other, less grave forms, suggesting that only the former gave rise to a right to self-defense.

<sup>70</sup>See the positions of Australia and Estonia, in 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 73/266, U.N. Doc. A/76/136 (Jul. 13, 2021).

<sup>71</sup>*Id.*

<sup>72</sup>See Wright, *supra* note 38.

<sup>73</sup>In case a cyber-attack is qualified as an armed or a terrorist attack, art. 42(7) Treaty on the European Union [hereinafter ‘TEU’] and art. 222 TFEU may be respectively triggered.

### E. The Strengthening of EU Powers to Attribute a Cyber-Attack: A Way Forward?

In Section C, we have seen that the EU's interest in cybersecurity is relatively recent. However, the number and the quality of EU-derived obligations for Member States has constantly grown since 2008. Several strategies were developed in 2013, 2017 and 2020 to tackle these security threats. Various instruments were deployed by EU to boost Member States' response capacity.<sup>74</sup> The most important is Directive (EU) 2016/1148<sup>75</sup> which was adopted in order to harmonize the security requirements of network and information systems ('NIS') against which cyber-attacks might be directed. This piece of legislation laid down minimum harmonization requirements and introduced obligations concerning security measures and incident notifications across sectors which are vital for the economy and society.<sup>76</sup> The objective of this measure was to achieve a high common level of security of network and information systems and was designed to enhance strategic and operational cooperation between Member States. The rationale for the adoption of Directive 2016/1148 was to prevent that cyber-attacks could have serious disruptive effects affecting more than one Member State, thus hampering the functioning of the internal market.<sup>77</sup> Yet, this legislation was too limited. This is why in 2020 the Commission proposed to expand the harmonization requirements of the NIS Directive and to increase the number of sectors subject to it.<sup>78</sup>

At the same time, in December 2020, an amendment to the "ECI" Directive<sup>79</sup> was also put forward. The proposed new rules are aimed at increasing resilience of "critical entities"<sup>80</sup> by extending the application of the Directive, which initially covered the energy and transport sectors, to banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure, public administration, and space. The proposed rules seek to "enhance the resilience of entities in the Member States which are critical for the provision of services which are

<sup>74</sup>The EU Cyber Defence Policy Framework (CD Policy Framework) was established in 2014. See *EU Cyber Defence Policy Framework*, COUNCIL OF THE EU (Nov. 18, 2014), <https://ccdcoe.org/uploads/2018/11/EU-141118-EUCyberDefencePolicyFrame-2.pdf>. See also Jed Odermatt, *The European Union as a Cybersecurity Actor*, ICOURTS WORKING PAPER SERIES 14 (2018). The first priority was to support the development of Member States' cyber defense capabilities related to CSDP.

<sup>75</sup>See Council Directive 2016/1148, 2016 O.J. (L 194).

<sup>76</sup>For example, Member States must identify operators of essential services and adopt a national strategy on the security of network and information systems; they must also designate one or more national competent authorities on the security of network and information systems with the task of monitoring the application of the Directive.

<sup>77</sup>However, under Council Directive 2016/1148, *supra* note 75, at art 1(6), Member States have the power to safeguard their essential State functions, in particular to safeguard national security.

<sup>78</sup>A proposal for an amendment of this Directive was recently put forward by the Commission. See *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) No. 2016/1148*, EUR-LEX (Dec. 16, 2020), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN>. The aim is to extend the number of sectors covered by the 2016 Directive as in the assessment of the Commission there would currently be more digitised sectors providing key services to the economy than in 2016. Furthermore, it is underlined that the Directive in its original version granted Member States a wide discretion in setting security and incident reporting requirements for operators of essential services; however, this has resulted in a great inconsistency of rules at national level and has caused additional costs and has created difficulties for companies offering cross-border goods or services.

<sup>79</sup>See Council Directive 2008/114, 2018, *supra* note 45. This piece of legislation is aimed at protecting the infrastructure that enables the provision of essential services or functions for society or economic activities. It was a first step to identify and designate ECIs whose disruption caused by attacks had significant cross-border impacts (on at least two Member States). The overall objective of the Directive was to increase the critical infrastructure protection capability in Europe which could be the object of man-made and technological threats such as terrorist and cyber-attacks and also natural disasters.

<sup>80</sup>See *Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities*, EUR-LEX (Dec. 16, 2021), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0829>. On May 13, 2022, the Commission has announced that a political agreement was found between the Parliament and the Member States on the final text of the Directive. See *Commission Welcomes Political Agreement on New Rules on Cybersecurity of Network and Information Systems*, EUROPEAN COMMISSION (May 13, 2022), <https://digital-strategy.ec.europa.eu/en/news/commission-welcomes-political-agreement-new-rules-cybersecurity-network-and-information-systems>.

essential for the maintenance of vital societal functions or economic activities in the internal market in a number of sectors underpinning the functioning of many other sectors of the economy of the Union.”<sup>81</sup> The idea behind the new rules is that considering the increased interdependency between services provided using critical infrastructure in the sectors mentioned above, a disruption in one Member State may have implications in other EU members or the whole EU. The divergence of regulations at national level is a factor that obstructs the functioning of the internal market and makes the Union more vulnerable in terms of security. Harmonizing the security requirements, which should be respected by critical entities providing essential services, is necessary. The proposed directive sets up a procedure for Member States to identify critical entities using common criteria on the basis of a national risk assessment and sets out a number of obligations on Member States.

The EU is clearly enhancing the security requirements that the mentioned infrastructure should respect and will continue to do so in the future, considering that the effects of cyber-attacks may either hamper the functioning of the internal or undermine the security of the Member States, that of the Union and international security. Given the *unique* level of integration of the EU and the specific solidarity mechanisms amongst the Member States, provided for by the EU Treaties,<sup>82</sup> the EU has an interest in addressing the lack of capacity of several of its members to identify and respond to cyber-attacks. In addition, the dependency on the intelligence of the US and United Kingdom (UK) as far as the attribution to third states of a cyber-attack is problematic. In this context, it is submitted that the EU could contribute to address the “special attribution problems” created by cyber-attacks, thus identifying an attribution mechanism enabling the organization, as a subject of international law, to trigger state responsibility in the event a cyber-attack targets the territories of one of its Member States. It may be wondered whether the EU has also the ability to carry out this task. In principle the answer is positive. Indeed, on the one hand, the EU has strengthened its research and technological capacities to secure network and information systems, and in particular to protect critical network and information systems because this is in the Union’s strategic interest.<sup>83</sup> On the other hand, the EU institutional set up was reinforced. In 2019 a specific body, the European Union Agency for Cybersecurity (ENISA),<sup>84</sup> which was created in 2013, was entrusted amongst other tasks, to assist the Member States and the EU institutions to prevent, detect and improve their capabilities to respond to cyber threats and incidents.<sup>85</sup> The Agency also plays an important role in assisting national authorities to develop strategies on the security of network and information systems and, broadly speaking, in implementing Directive 2016/1148.<sup>86</sup> In principle, this body does not have an autonomous capacity to make the technical determination necessary to attribute a certain cyber conduct to a given threat source.

The mentioned EU organ assists both the Member States and the EU institutions and is considered as “a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers, the information it provides.”<sup>87</sup> The Agency may, at the request of one or more Member States, “provide support in relation to ex-post technical inquiries regarding incidents having a significant or substantial influence within the meaning of Directive (EU) 2016/1148.”<sup>88</sup> It is submitted that these powers could be used and further expanded through a change of the Regulation instituting this agency to develop,

<sup>81</sup>See *Proposal for a Directive of the European Parliament*, *supra* note 78, at 4.

<sup>82</sup>See Comments, *supra* note 73.

<sup>83</sup>See Council Regulation (EU) No. 2021/887, O.J. 2021 (L 202), recital n. 6.

<sup>84</sup>See Council Regulation (EU) No. 2019/881, O.J. 2019 (L 151). The Agency was set up with Council Regulation (EU) No. 526/2013, O.J. 2013 (L 165).

<sup>85</sup>See *id.* at art. 6(1)(a) and (c).

<sup>86</sup>See *id.* at art. 5(2).

<sup>87</sup>*Id.* at art. 4(1).

<sup>88</sup>*Id.* at art. 7(3)(d).

in cooperation with national authorities, an attribution mechanism of cyber-attacks to a third state. If this were to happen, the EU would achieve a double purpose: on the one hand, it would address the problem of those EU members that lack capacity and expertise in this area; on the other hand, it could provide a model for technical attribution to be adopted or adapted by the international community.

Yet, there are a number of legal and political obstacles to the expansion of the EU Cybersecurity agency's tasks. Indeed, the delegation of powers to agencies is subject to the constraints of the *Meroni*<sup>89</sup> case-law: first, agencies may be delegated only executive powers while discretionary powers have to be exercised by the delegating authority; second, the latter cannot delegate broader powers than it enjoys itself. While the technical attribution of responsibility may be seen as an executive power, it is not clear whether the EU would have the competence to attribute state responsibility to a third country. This is the reason why the Agency could not be given powers to define an attribution mechanism. Yet, the legal framework is uncertain. It could be counterargued that given that the requirements of the "*Meroni* doctrine" have been made less stringent by the Court of Justice with the *ESMA* ruling,<sup>90</sup> it is possible to enshrine on the Cybersecurity Agency more powers, provided that the latter are clearly defined, as required by the ECJ.<sup>91</sup> Therefore, the legal obstacle to expanding EU Agency's powers would be overcome; it goes without saying that Member States would have to agree on taking such a step and this is a political decision.

At the same time, other platforms could be equipped with powers to attribute cyber-attacks. In this respect, it is interesting that the Commission recommended to build the Joint Cyber Unit and to set it up in a 4-step process that will include the identification of the EU available operational capabilities, the preparation of incident and crisis response plans at national and EU levels, and expansion of activities to establish cooperation with private entities. The operationalization of the Joint Cyber Unit is expected to be completed by 30 June 2023.<sup>92</sup> It should be noted that in an annex to the recommendation on building a joint cyber unit, it is envisaged that this unit may be used "by the cyber diplomacy community to align public communication. The platform may allow participants to contribute to political attribution as well as attribution within the criminal justice framework employed at police and judicial level."<sup>93</sup> In addition, it may facilitate recovery and allow for structured synergies with national and cross-border monitoring and detection capabilities that participants to coordinate public communication and contribute to political attribution, as well as attribution in the context of the criminal justice. However, in the EU's Cybersecurity Strategy for the Digital Decade it is also confusingly stated that this platform "would not be an additional, standalone body, nor would it affect the competences and powers of national cybersecurity authorities or EU participants."<sup>94</sup> Be as it may, should the organization be able to make the decision to extend ENISA's powers or to set up the new cyber unit, the decisions on attribution of cyber-attacks would be recognized by the EU Member States but certainly not by third countries. This is an important limit. Therefore, developing the powers of new Union bodies would serve to enhance the ability of the Member States to attribute cyber-attacks and

<sup>89</sup>See Case C-9/56, *Meroni & Co. v. High Authority of the Eur. Coal and Steel Cmty.*, 1958 E.C.R. 133.

<sup>90</sup>See Case C-270/12, *U.K. of Gr. Brit. and N. Ir. v. Eur. Parl. and Council*, ECLI:EU:C:2013:562 (Jan. 20, 2014). If delegation of powers complies with the legal guarantees set by the amended Treaties, the Court sees no objections to have delineated but discretionary powers conferred upon agencies. This is the lesson to be drawn from the *ESMA* ruling. See Ellen Vos, *EU Agencies on the Move: Challenges Ahead*, SIEPS 31 (2018), <https://www.sieps.se/en/publications/2018/eu-agencies-on-the-move-challenges-ahead/>.

<sup>91</sup>See Joined Cases C-154/04 & C-155/04, *Nat'l Assoc. of Health Stores v. Sec'y of State for Health*, 2005 E.C.R. I-06451.

<sup>92</sup>See Commission Recommendation 2021/1086 of 23 June 2021 on building a Joint Cyber Unit, 2021 O.J. (L237), at 9.

<sup>93</sup>See *Annex to the Commission Recommendation on Building a Joint Cyber Unit*, COM (2021) 4520 final (Jun. 23, 2021), at 12.

<sup>94</sup>See *Joint Communication to the European Parliament*, *supra* note 44, at 14.

to take a common decision within the EU. Yet, it would not provide a universally acceptable verification mechanism.

## F. Final Remarks

Because States are reluctant to establish a comprehensive legal framework to counter cyber-attacks, this hints at a tendency of informalization and flexibility of regulation that one can observe in other areas related to digitalization as well. This also happens in the EU context. The organization is ready to impose cyber sanctions on individuals, including *de jure* state organs, but not to trigger the rules on international legal responsibility. We consider that the main reason for the inclusion of the clause in Recital n. 9 is that there is a reluctance by Member States to let that the EU engage state responsibility. However, the choice of the Council may also be due to the inherent difficulties in attributing a cyber-attack to a given actor, which prompted its explicit decision to leave this task to Member States. Significantly, in other cases of restrictive measures addressing non-digital threats, the Union had never openly affirmed that legal attribution should be left only to Member States.

To address the challenges posed by malicious cyber activities some have proposed to set up a widely accepted attribution mechanism.<sup>95</sup> Yet, at the moment, EU Member States (but more broadly the international community) do not seem to have an interest towards the establishment of a technical verification mechanism which could only be fully legitimized if all main state actors would agree to its establishment and possibly contribute to its running. Major cyber actors, notably China, have shown little enthusiasm for this initiative and suggest (rather opportunistically) that “attribution is nearly impossible.”<sup>96</sup> Without China and its allies on board the credibility of the independent entity would be severely undermined.

At the same time, it was suggested that more specific rules of attribution of conduct and responsibility that would apply to the cyber domain should be developed (or are indeed emerging from State practice).<sup>97</sup> According to this proposal, States should be able to attribute unlawful cyber operations of non-State actors to States, even in the absence of evidence demonstrating clear State direction and control. While such a special regime would technically be possible under the law on State responsibility,<sup>98</sup> there seems to be little state practice upon which these special rules should rest. States are only now beginning to set forth their views on how international law governs cyberspace, but too few of them have made their approach clear and they are still overshadowed by the number of States that are reticent to do so. As evidenced above, so far States have not been inclined to develop public and shared rules for attributing cyber-attacks and prefer to take advantage of a regulative gap that allows them to react to cyber incidents as they see fit (and perhaps to carry out hostile cyber operations themselves).<sup>99</sup> The EU

<sup>95</sup>A possible model is the verification mechanism enabling the identification of the State responsible for using prohibited chemicals weapons. The Organization for the Prohibition of Chemical Weapons (OPCW) is tasked with ensuring the implementation of the Convention and with verifying the compliance with the CWC. See Yuval Shany & Michael N. Schmitt, *An International Attribution Mechanism for Hostile Cyber Operations*, 96 INT'L L. STUDS. 196, 221 (2020) (supporting the idea of an independent international attribution mechanism for cyber operations along the lines of the OPCW's Technical Secretariat).

<sup>96</sup>See Michael Sulmeyer & Amy Chang, *Three Observations on China's Approach to State Action in Cyberspace*, LAWFARE BLOG (Jan. 22, 2017), <https://www.lawfareblog.com/threeobservations-chinas-approach-state-action-cyberspace>.

<sup>97</sup>See Peter Z. Stockburger, *Control and Capabilities Test: Toward a New Lex Specialis Governing State Responsibility for Third Party Cyber Incidents*, 9th Int'l Conference on Cyber Conflict, 1–14 (2017) (transcript available at <https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf>).

<sup>98</sup>See ARSIWA, *supra* note 26, at art. 55. Titled *lex specialis*, states that the articles “do not apply where and to the extent that the conditions for the existence of an internationally wrongful act or the content or implementation of the international responsibility of a State are governed by special rules of international law.”

<sup>99</sup>See Finnemore & Hollis, *supra* note 56, at 997–1000.

itself has never advocated for structural changes of international law as far as the attribution mechanism of cyber activities is concerned.<sup>100</sup>

However, the idea of concluding binding agreements of a more limited scope to regulate State behavior in the cyber domain should not be entirely abandoned.<sup>101</sup> While a treaty on general rules of conduct would require a political will that is currently lacking, steps forward could be made on banning or regulating specific areas, such as commercial cyber espionage or malicious cyber-activities against critical infrastructure.<sup>102</sup> The prospect of having to cope with huge financial and reputational costs might pave the way for the adoption of more specific treaties which could also establish rules and procedures regulating issues of attribution and responsibility that could serve as models for other similar exercises. Meanwhile, it is to be hoped that the severity of hostile cyber operations remains under the threshold of what could be regarded as an armed attack, as otherwise the described normative ambiguity could dramatically backfire.

**Acknowledgement.** The authors thank the editors of the present issue for their most helpful comments. All errors remain, of course, our own.

**Competing Interests.** None.

**Funding Statement.** No specific funding has been declared in relation to this article.

**Author's Note.** The two authors jointly conceived the ideas behind this article and have written Sections A and F together. Professor Poli has written Sections C and E, while Professor Sommario has written Sections B and D. This article reflects the state of developments as of August 25, 2022.

---

<sup>100</sup>The High Representative of the Union, Borrell, has stated in a speech that “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 (emphasis added) 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).” *Declaration by the High Representative on Behalf of the EU on Respect for the Rules-Based Order in Cyberspace*, COUNCIL OF THE EU (Apr. 12, 2019), <https://www.consilium.europa.eu/en/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/>.

<sup>101</sup>See Moynihan, *supra* note 22, at 55.

<sup>102</sup>See *Carnegie Endowment's Cyber Norms Index*, CARNEGIE ENDOWMENT FOR INT'L PEACE, <https://carnegieendowment.org/publications/interactive/cybernorms> (including a list of already existing bilateral and multilateral agreements (both binding and non-binding) on different aspects of cyber security).

**Cite this article:** Poli S, Sommario E (2023). The Rationale and the Perils of Failing to Invoke State Responsibility for Cyber-Attacks: The Case of the EU Cyber Sanctions. *German Law Journal* 24, 522–536. <https://doi.org/10.1017/glj.2023.25>