ARTICLES

# THE EXTERNALISATION OF THE EU'S CYBERSECURITY REGIME: THE CYBER DIPLOMACY TOOLBOX

YULIYA MIADZVETSKAYA* AND RAMSES A. WESSEL**



ABSTRACT: It is often claimed that there is a blurring line between external and internal security in the EU with both being increasingly intertwined. Apart from providing the state of affairs in EU cybersecurity law and policy, the argument of this contribution is that these internal-external links are also visible in a growing tendency towards the *externalisation* of the EU's cybersecurity policy. Typical interior policy fields in that area that were tackled through the internal market and the Area of Freedom Security and Justice (AFSJ) legal bases, are now penetrating the field of action of the Common Foreign and Security Policy (CFSP). This tendency towards a growing *externalisation* of the EU cybersecurity will be demonstrated by analysing the emblematic EU's Cyber Diplomacy Toolbox and its deterrence instrument: restrictive measures in response to cyber-attacks. Our analysis pinpoints a number of limitations for the EU's common action under the CFSP, including problems of attribution and evidence collection. Our *Article* questions whether the CFSP is fit for the digital age and what repercussions cyber threats may have for the future of the EU CFSP and its Cyber Diplomacy Toolbox.

KEYWORDS: Cyber Diplomacy Toolbox – CFSP – restrictive measures – PESCO – sanctions – cybersecurity.

* Researcher at the Chair of Law and Artificial Intelligence, University of Tuebingen, yuliya.miadzvetskaya@uni-tuebingen.de.

** Professor of European Law, Faculty of Law, University of Groningen, r.a.wessel@rug.nl.
Yuliya Miadzvetskaya is the first and main author of this *Article*. This research was funded by the *Deutsche Forschungsgemeinschaft* (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC number 2064/1 – Project number 390727645.


ISSN 2499-8249
doi: 10.15166/2499-8249/570

## I. Introduction

There is nothing new in stating that both European and national institutions are increasingly confronted with new cyber threats. Throughout 2021 the European Medicines Agency and the European Banking Authority have both been subject to cyber-attacks.[1] At national level, in May 2021 a ransomware attack affected the Irish health sector.[2] In Belgium two large scale cyber-attacks hit Belnet and the Internal Affairs Department responsible for immigration policy and public order.[3] In February 2022 cyber-attacks hit oil facilities in Belgium, Germany and the Netherlands.[4] And the year 2022 started with a series of cyber-attacks on Ukraine[5] followed by the Russian aggression through kinetic warfare.

Against this background, the resilience of institutions and critical infrastructures to cyber threats is of paramount importance to the EU and its partner countries. Security is one of the core objectives of the EU mentioned both in provisions relating to the Area of Freedom, Security and Justice (AFSJ) and the Common Foreign and Security Policy (CFSP). Traditionally, there has been a divide in the EU between internal security issues falling under the AFSJ (such as crime, terrorism, racism, xenophobia)[6] and the external dimension of the EU's security covered under the CFSP. The latter were, and to a large extent still are, "subject to specific rules and procedures",[7] and it remains complex to adopt measures combining them. Furthermore, art. 4(2) TEU – the *national identity clause* – requires the EU to respect some core areas of "Member States' national identities" and "essential State functions", including national security. The *national identity clause* is meant to preclude an "encroachment" of the EU upon Member States competences, in particular upon Member States' freedom to determine the requirements of public policy and security in accordance with their national needs.[8] In addition, art. 72 TFEU prevents the EU's action in the AFSJ from interfering with the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security.

These days, the notion of EU security changes in fundamental ways along with the nature of threats due to the emergence of new technologies. The EU has been increas-

[1] A Neville, 'Recent Cyber-Attacks and the EU's Cybersecurity Strategy for the Digital Decade' (2011) European Parliament Research Service.

[2] *Ibid.,* 1.

[3] *Ibid.*

[4] J Tide, 'European Oil Facilities Hit by Cyber-Attacks' (3 February 2022) BBC www.bbc.com.

[5] For a detailed account of cyber aspects of the Russian war in Ukraine see B Smith, 'Defending Ukraine: Early Lessons from the Cyber War' (22 June 2022) Microsoft aka.ms; L Harding, 'Ukraine Hit By "Massive" Cyber-Attack on Government Websites' (14 January 2022) The Guardian www.theguardian.com.

[6] Art. 67(3) TFEU.

[7] Art. 24(1) TEU.

[8] Case C-348/09 *P.I. v. Oberbürgermeisterin der Stadt Remscheid* ECLI:EU:C:2012:300 para 23.

ingly exposed to hybrid threats in the last years.[9] This contribution aims to look at one of the pressing issues of EU security: cybersecurity. It aims to unveil the tendency towards the *externalisation* of EU cybersecurity concerns. By *externalisation* we understand an increase in institutionalised forms of joint representation or joint initiatives of the EU vis-à-vis external actors in the field of cybersecurity.

For instance, some EU Member States, notably Estonia, France, Germany, the Netherlands, and Romania participate in discussions of the UN Group of Governmental Experts (UNGGE) on non-binding normative agreements for cyberspace. The new mandate of the UNGGE also provides for informal consultations with regional organisations, including the EU.[10] A parallel process on responsible State behaviour in cyberspace takes place within the Open-Ended Working Group (OEWG) open to all the UN members. In addition to this, the EU is also involved in negotiations on the updating of Budapest Convention on Cybercrime within the Council of Europe[11] as well as on a new Convention on the use of information technology and communications technologies for criminal purposes at the UN.[12] The EU's participation in multilateral negotiations on cyber norms at different international fora takes place along with the launch of the EU's unilateral initiatives such as Cyber Diplomacy Toolbox in 2017[13] and the first enactment of sanctions in response to cyber-attacks in 2020.[14]

The growing ambition of the EU as a global cyber actor[15] called for a less inward-looking approach towards cyber-incidents and for a more outward-looking EU. Practically this translates in a shift from the conventional defence of networks and resilience-building paradigm to the EU that promotes and enforces norms of responsible State behaviour across its borders.

Cybersecurity, by definition, often transcends national, international, transnational and private actors, both internally and externally. This lies behind the ongoing discus-

[9] L Lonardo, 'EU Law Against Hybrid Threats: A First Assessment' (2021) European Papers www.europeanpapers.eu 1075.

[10] Group of Governmental Experts**,** Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security A/76/135, para 4.

[11] Council of Europe, Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence [2022].

[12] General Assembly, Resolution 75/282 of 26 May 2021, UN Doc A/RES/75/282.

[13] Council, Conclusions of 19 June 2017 on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"); Council, Draft implementing guidelines of 9 October 2017 for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities.

[14] 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; 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.

[15] RA Wessel, 'European Law and Cyberspace' in N Tsagourias and R Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2021) 490.

sion on the blurring divide between the external and internal dimensions of security,[16] in which the argument often is that security *at home* cannot be guaranteed without addressing the root causes of security challenges abroad.[17] This is even more so taking into account the EU's offer to provide cyber support to Ukraine[18] by a group of EU countries that launched the Cyber Rapid Response Team (CRRT) under the PESCO cooperation scheme.[19] As a side note, the CRRT was not deployed in Ukraine since the context has changed dramatically after the start of the Russian invasion of Ukraine.[20] The question remains, however, to what extent the EU is legally, functionally and operationally endowed to counter external cyber threats.

EU cybersecurity initiatives were initially developed as measures aimed at establishing and securing a well-functioning internal market.[21] For instance, the NIS Directive, a central piece of the EU's cybersecurity-related legal framework, mentions the "achievement of a high common level of security of network and information systems within the Union"[22] as one of the essential objectives necessary for the smooth functioning of the internal market. Step by step, cybersecurity issues were tackled also under the AFSJ and some other perhaps less expected legal provisions relating to for instance research and technological development and industry.[23]

However as from 2013, the *externalisation* of EU cybersecurity and its mainstreaming into EU foreign policy, notably the CFSP, was announced by the EU Cybersecurity Strate-

[16] X Kurowska and P Pawlak, 'Introduction: The Politics of European Security Policies' (2009) Perspectives on European Politics and Society 474; J Eriksson and M Rhinard, 'The Internal-External Security Nexus' (2009) Cooperation and Conflict 243.

[17] P Pawlak, 'The External Dimension of the Area of Freedom, Security and Justice: Hijacker or Hostage of Cross-Pillarization?' (2009) Journal of European Integration 25, 35.

[18] L Cerulus, 'EU Races to Help Ukraine Fight Cyberattack" (14 January 2022) Politico www.politico.eu.

[19] LRT, 'Lithuania May Activate EU Cyber Force to Help Ukraine' (17 January 2022) LRT www.lrt.lt.

[20] Exchanges on Twitter with Laurens Cerulus, Cybersecurity Editor at Politico Europe. The exchange is publicly accessible here: www.twitter.com.

[21] Research on the EU law aspects of cybersecurity is limited, but see J Odermatt, 'The European Union as a Cybersecurity Actor' in S Blockmans and P Koutrakos (eds), *Research Handbook on EU Common Foreign and Security Policy* (Edward Elgar Publishing 2018) 354; A Bendiek and E Pander Maat, 'The EU's Cybersecurity Policy: Building a Resilient Regulatory Framework' in G Siboni and L Ezioni (eds) *Cybersecurity and Legal-Regulatory Aspects* (World Scientific 2021) 23; as well as RA Wessel, 'European Law and Cyberspace' cit. 15.

[22] 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 ("NIS Directive"), art. 1.

[23] Arts 173(3) and 188 TFEU served as legal bases for establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres; art. 173(3) TFEU provides for measures to support the competitiveness of the Union's industry; art. 188 TFEU defines a procedure for setting up joint undertakings for the Union's research, technological development and demonstration programmes.

gy.[24] Since 2015 the Council's conclusions started shaping what is now called *EU cyber diplomacy* by highlighting the need for cooperation with third countries, industry, academia and civil society for establishing a coherent cyberspace policy.[25] In October 2017, EU Member States adopted a Cyber Diplomacy Toolbox that laid down foundations for a joint EU diplomatic response to malicious cyber behaviour.[26] The 2019 Cybersecurity Act also recognised the need for EU wide response to cyber-attacks. According to the Cybersecurity Act, there is a need to overcome the problem that cybersecurity and law enforcement authorities are predominantly national, whereas large-scale incidents necessitate effective and coordinated responses and crisis management at Union and global levels.[27]

Earlier, a similar development could be also observed with respect to other security threats, such as terrorism, which led to the *externalisation* of the AFSJ and its penetration into issues of EU foreign policy.[28] With respect to EU cybersecurity, internal rule-making also proves inseparable from EU external rule-making.

This *Article* demonstrates how, after having started as an element of the internal market, cybersecurity now found a solid anchor in the CFSP. The Cyber Diplomacy Toolbox and cyber-sanctions will be examined as a case-study for showcasing the emergence of EU initiatives in the field of the CFSP. By connecting the dots between different legal instruments in the field of cybersecurity, this *Article* aims to shed light on the main developments in the EU cybersecurity legal framework. First, it points to cybersecurity as an internal market initiative (section II). Secondly, it zooms in on the role of the AFSJ in further shaping the EU cybersecurity framework (section III). It concludes with an analysis of the *externalisation* of EU cybersecurity through the CFSP and the special role this policy area plays in a further development of EU cybersecurity (section IV). In this contribution we aim to go beyond the law in books and explore how the ambitions stated in EU official documents correspond to what the EU is functionally and operationally endowed to do (section V).

[24] Joint Communication JOIN/2013/01 final from the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy of 7 February 2013, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace' ("The EU 2013 Cybersecurity Strategy").

[25] Council, Conclusions on Cyber Diplomacy 6122/15, 11 February 2015.

[26] Council, Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities cit.

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

[28] C Matera, 'Some Reflections on the Nature and Scope of the Externalisation of the AFSJ Domains' in M Fletcher and E Herlin-Karnell (eds) *The European Union as an Area of Freedom, Security and Justice* (Routledge 2016) 357.

## II. Cybersecurity as internal market resilience

Several cybersecurity related initiatives have been addressed on the basis of the internal market clause of art. 114 TFEU. As is well known, under this provision, the EU can adopt measures for the approximation of national laws, regulations and administrative practices with the objective of establishing the internal market and enabling its functioning (*harmonisation*). Unlike other policy areas, the internal market is not determined by one concrete policy field. Some scholars note that art. 114 TFEU endows the Union with functional powers, as an expression of an open-ended integration, and deliberately broadly formulated in view of the necessary flexibility.[29]

In the absence of an explicit legal basis to regulate cybersecurity, the economic rationale of the internal market clause was relied upon as one of the most appropriate legal bases for bringing security, resilience and trust to the EU digital market.[30] The EU Digital Single Market Strategy identified secure and trustworthy infrastructures as necessary conditions for maximising the growth potential of the digital economy.[31] Since cyber threats are a borderless problem, extending beyond the boundaries of any Member State, they may lead to significant economic losses. Therefore, cybersecurity considerations call for the EU-wide action, for more harmonisation and integration. Conversely, diverging cyber regulations risk having negative effects on the functioning of internal market and the overall coherence of EU policies.

The internal market clause bears a lot of uncertainty with respect to its area of application.[32] The appropriateness of this provision for intervening in (cyber)security-related matters is questionable from the point of view of both the vertical and horizontal distribution of competences. The broader the scope of art. 114 TFEU, the larger the *creeping expansion* of EU competences to the detriment of Member States' powers.[33] While it is obvious that the well-functioning internal market is unthinkable without secure infrastructures, it remains unclear how far the EU can go with this provision in order to address a growing number of hybrid threats.

In the past many have accused the EU of the inappropriate use of the free movement provisions where "Union competence is either non-existent, severely circumscribed or subject to very different institutional arrangements".[34] A balanced guidance on the operation of art. 114 TFEU was offered in the *Tobacco Advertising Directive* ruling, establishing that proposed measures should have a meaningful and demonstrable

[29] S Garben, 'Confronting the Competence Conundrum: Democratising the European Union Through an Expansion of its Legislative Powers' (2015) OJLS 55, 74.

[30] RA Wessel, 'European Law and Cyberspace' cit. 15. See also art. 1 NIS Directive cit.

[31] Communication COM(2015) 192 final from the Commission of 6 May 2015 'A Digital Single Market Strategy for Europe'.

[32] M Dougan, 'Legal Developments' (2010) JComMarSt 163, 164.

[33] S Garben, 'Confronting the Competence Conundrum' cit. 70.

[34] M Dougan, 'Legal Developments' cit. 172-173.

connection to the internal market.[35] The subsequent case-law has adopted a broader interpretation of art. 114 TFEU by abandoning the requirement for "an actual link with free movement between the Member States" in favor of a more relaxed test such as the general intention of the measure to improve the functioning of internal market.[36] The expansionist reading of art. 114 TFEU was a key trend of the case-law after the first *Tobacco Advertising Directive* ruling.[37]

A high common level of security of network and information systems is one of the essential elements of a smooth functioning internal market.[38] This tendency towards the (cyber)securitisation of the internal market legal basis is not recent. The internal market clause was already relied upon for establishing the EU Agency for Cybersecurity (original name: European Network and Information Security Agency (ENISA)) in 2004. The appropriateness of the internal market legal basis for enacting cyber related legislation has been upheld by the Court of Justice in 2004[39] when the United Kingdom contested the use of art. 114 TFEU for the establishment of the ENISA. According to the UK, the power delegated to the EU is the power to harmonise and not to set up new bodies. The Court did not agree. Art. 114 TFEU played a crucial role in the agencification of EU policies "in particular in fields with complex technical features".[40] The relevance of the internal market legal basis for establishing the ENISA was further confirmed by the 2013 Regulation (EU) No 526/2013 establishing the new mandate of the Agency for a period of seven years and the 2019 Cybersecurity Act which provides for the permanent mandate of the Agency.

Furthermore, the landmark judgment in *Digital Rights Ireland* confirmed that several security-oriented purposes such as the prevention, investigation, detection and prosecution of serious crimes, can be addressed under the internal market harmonisation competence of art. 114 TFEU.[41] The Directive on security of network and information systems (NIS),[42] a central piece of the EU's cybersecurity-related legal framework, also finds its legal basis in internal market harmonisation provisions. The NIS Directive and its updated

[35] *Ibid.* 173; Case C-376/98 *Germany v. European Parliament and Council* ECLI:EU:C:2000:544, paras 83-84.

[36] Joined Cases C-465/00 C-138/01 & C-139/01 *Rechnungshof v. Österreichischer Rundfunk* ECLI:EU:C:2003:294, para 41. Case C-380/03 *Germany v. Parliament and Council* ECLI:EU:C:2006:772, para 80; See also Case C-491/01 *British American Tobacco (Investments) and Imperial Tobacco* ECLI:EU:C:2002:741, para 60.

[37] SR Weatherill, 'The Limits of Legislative Harmonisation Ten Years after Tobacco Advertising: How the Court's Case Law has Become a "Drafting Guide"' (2011) German Law Journal 827.

[38] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final, 7 February 2013.

[39] Case C-217/04 *United Kingdom vs. European Parliament and Council* ECLI:EU:C:2006:279.

[40] Case C-358/14 *Republic of Poland v European Parliament & Council* ECLI:EU:C:2016:323, para. 68; M Chamon and V Demedts, 'Constitutional Limits to the EU Agencies External Relations' in H Hofmann, E Vos, and M Chamon (eds) *The External Dimension of EU Agencies and Bodies* (Edward Elgar Publishing 2019) 12.

[41] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* Ltd ECLI:EU:C:2014:238, para 24.

[42] NIS Directive cit.

version NIS2 Directive[43] lay down a common EU legal framework regarding Member States capabilities in handling network and information systems incidents, mechanisms for EU-wide cooperation and requirements for key private and public actors. The European Cyber Resilience Act on common cybersecurity standards for connected devices[44] and the European Chips Act,[45] that are expected to already rely on art. 114 TFEU.

At the same time, the recourse to 114 TFEU legal basis for cybersecurity-related purposes comes with several limitations. Network and information systems, communications networks, digital products, services and devices support our everyday societal activities. The danger of using internal market provisions for regulating cross-cutting policy issues with an important human dimension resides in their primarily economic policy-aims to the detriment of other objectives. This economic bias in the adoption of legislative measures entails the risks of overlooking or undervaluing other socio-cultural values at stake.[46] At the same time, different provisions scattered throughout the Treaties make it compulsory for internal market legislation to take other non-related objectives on board.[47] A classic example of this reasoning is the Directive on Audiovisual Media Services, which is grounded in the internal market objective of facilitating the provision of media services and *inter alia* constitutes a cultural policy instrument of promotion of European programmes.[48] The EU Cybersecurity Act, referring to the importance of cybersecurity awareness-raising and education, could qualify as another example of an incorporation of non-market objectives in the measures based on art. 114 TFEU. Even if the internal market clause is relied upon for legislating non-market aims, pursuing those non-economic objectives can have an economically beneficial effect.[49]

As was shown above, the internal market legal basis was relied upon on several occasions as an appropriate legal basis for building a more coherent EU approach to handle cyber incidents. Indeed, divergences in cyber capabilities between Member States and levels of protection across the EU could endanger, in turn, the functioning of the

[43] Commission 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, 16 December 2020 ("NIS 2 Directive").

[44] The European Cyber Resilience Act is being in preparation with the Commission's proposal foreseen for the third quarter of 2022.

[45] Proposal for a Regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act), COM(2022) 46, 8 February 2022. The European Chips Act is meant to develop Europe's semiconductor industry, making it less dependent on international supply chains.

[46] S Garben, 'Confronting the Competence Conundrum' cit. 69.

[47] B de Witte, 'A Competence to Protect: The Pursuit of Non-Market Aims Through Internal Market Legislation' in P Syrpis (ed), *The Judiciary, the Legislator and the Internal Market* (CUP 2012) 25, 32. For instance, the values and objectives of gender equality (art. 8 TFEU), non-discrimination generally (art. 10 TFEU), social protection (art. 9 TFEU) and animal welfare (art. 13 TFEU).

[48] *Ibid*. 34.

[49] *Ibid.* 26.

internal market. Furthermore, a comprehensive approach at Union level is necessary for preventing incidents causing disruption of IT services and critical infrastructures.[50]

It is not excluded that in future art. 114 TFEU could be relied upon to incentivise Member States to share more information and for expanding EU institutions' powers in terms of cyber threat analysis sharing. As a consequence, this would help bridging the existing gap between external and internal dimensions of (cyber)security. The use of art. 114 TFEU for addressing cybersecurity implications is reminiscent of the EU's practice to regulate social, regional development and environmental measures on the basis of the general harmonisation power conferred by internal market clause in the absence of sector-specific Treaty provisions in the past.[51] The number of legislative measures based on the internal market clause decreased with the creation of legal bases for sector-specific policies. We will see whether the overreliance on the internal market clause for (cyber)security related objectives could jumpstart a discussion on the reform of EU treaties and enhance cooperation in security and defence sectors, despite traditional Member States' reservations in the area. In this respect, the Russian aggression towards Ukraine served as a trigger for the security and defence dimension of the EU.

## III. Cybersecurity as an issue of internal security under the AFSJ

The AFSJ serves as another major legal anchor for bringing minimal harmonisation of sanctions for particularly serious crimes with a cross-border dimension to the cyber domain, as well as for the admissibility of cross-border evidence (art. 82(2) TFEU).[52] In a way, the AFSJ offers an umbrella that could be used to regulate different questions relating to internal security, including terrorism and cybercrime. The EU has deployed several legislative and non-legislative actions aimed at preventing cybercrime and building capacity in law enforcement and the judiciary. Those legal acts include the 2001 Framework Decision on combating fraud and counterfeiting,[53] the 2005 Council Framework Decision on attacks against information systems,[54] the 2011 Directive on

[50] H Carrapico and B Farrand, 'Cyber-Crime as a Fragmented Policy Field in the Context of the Area of Freedom, Security and Justice' in A Ripoll Servent and F Trauner (eds), *Routledge Handbook on the Area of Freedom, Security and Justice* (Routledge 2018) 146.

[51] B de Witte, 'A Competence to Protect' cit. 30.

[52] RA Wessel, 'European Law and Cyberspace' cit. 15.

[53] Council Framework Decision 2001/413/JHA of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment. This Decision was repealed by the Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision (2019) 2001/413/JHA.

[54] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

combatting the sexual exploitation of children online and child pornography,[55] and the 2013 Cybercrime Directive.[56]

The Directive on combatting the sexual exploitation of children online and child pornography was adopted on the basis of arts 82(2) and 83(1) and aims at criminalising child sexual exploitation and sexual abuse which is most evident in child pornography having a considerable cross-border dimension. The Cybercrime Directive contributes to the judicial cooperation in criminal matters and was adopted on the basis of art. 83(1) TFEU. It provides for minimum rules on the definition of criminal offences and sanctions in response to attacks against information systems. Those include access to systems, systems interferences, data interference and can be criminalised with penalties from two to five years.[57] It also sets out a procedure in its art. 12 on the basis of which a Member State must inform the Commission how it establishes its jurisdiction over offences outside its territory.

The reduction of criminal activities performed with the involvement of computers and information systems as a primary tool or as a primary target remains one of regulatory goals for the EU. With this objective, the European Cybercrime Centre (EC3) was officially launched in 2013 within Europol. The EC3 is designed as the European focal point in the fight against cybercrime. Cybercrimes can be divided into the following categories: cyber-dependant, cyber-enabled, and computer dependant.[58] A comprehensive legal definition of *cybercrime* for the EU was not yet provided in EU secondary law.[59] And we would argue that this not really needed since the nature of cybercrime evolves daily, in contrast to EU legal frameworks that take years before coming into being.

Since electronic evidence is relevant in around 85 per cent of the total criminal investigations, the Commission put forward a proposal for an e-evidence framework for facilitating cross-border access to electronic evidence.[60] Two legislative proposals were

[55] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision (2011) 2004/68/JHA.

[56] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA ("Cybercrime Directive").

[57] Art. 9 Cybercrime Directive.

[58] J Clough, *Principles of Cybercrime* (CUP 2010).

[59] The EU 2013 Cybersecurity Strategy refers to cybercrime as "a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target [...] and which 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)".

[60] Commission Staff Working Document Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parlia-

presented in 2018 in order to enhance the cross-border gathering of electronic evidence: a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters[61] and a Directive on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.[62] The first legal act is meant to allow law enforcement authorities from one Member State to request a service provider established in another Member State to provide access to or preserve data needed for investigation and prosecution of crimes. This legal act complements the Directive regarding the European Investigation Order in criminal matters,[63] which did not contain any specific provision with respect to electronic types of evidence. Furthermore, for strengthening the existing judicial cooperation mechanisms the European Commission envisages the creation of a secure platform for the swift exchange of requests between judicial authorities within the EU.[64]

Art. 82(1) TFEU on judicial cooperation in criminal matters was relied upon as the legal basis for a Regulation on European production and preservation orders for electronic evidence in criminal matters. This article provides for the possibility to adopt measures for ensuring recognition of judgments and judicial decisions and facilitating cooperation between judicial authorities of the Member States in relation to proceedings in criminal matters and the enforcement of decisions. However, it seems that the Regulation on European production and preservation orders for electronic evidence in criminal matters goes way beyond a mere judicial cooperation and mutual recognition rationale. It foresees rules on direct cooperation with service providers allowing the authority in one Member State to directly address the service provider in another Member State and even impose obligations on it. It follows that the procedures mentioned in the e-evidence framework do not involve two judicial authorities as laid down under art. 82(1) TFEU. It seems that the Commission in its proposal applies a certain degree of elasticity by using this provision for establishing a cooperation between law enforcement authorities and electronic services providers. The Regulation shifts away from the traditional application of the principle of mutual recognition in criminal matters and the case is yet another example of a creative use of existing legal bases by the Commission.

ment and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, SWD(2018) 118 final, 17 April 2018.

[61] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, 17 April 2018.

[62] Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM(2018) 226 final, 17 April 2018.

[63] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.

[64] Proposal COM(2018) 225 final cit.

As noted above, internal rule-making in the EU is inseparable from external rule-making.[65] This statement can be confirmed by the observation on the evolution of the *ERTA* doctrine and its role in EU external relations law.[66] Something that starts as an EU internal policy area will sooner or later have consequences for the EU's external action or will simply develop an external dimension. This is also clearly visible in the area of the AFSJ with respect to cybercrime.[67]

As most of the world's information is now stored digitally, it is hard to imagine a criminal investigation that does not involve digital evidence. Indeed, the cross-border access to electronic evidence is a pressing issue in 55% of crimes investigation and prosecution.[68] Furthermore, the efficiency of gathering e-evidence through legal agreements is, however, questionable since it often entails complex lengthy procedures. As a result, governments tend to opt for extraterritoriality of their access request and compel companies under their jurisdiction to grant access to data regardless of the location of the servers.[69] Since September 2019 the EU has been negotiating an agreement with the US on access to e-evidence for judicial cooperation in criminal matters.[70] The Commission plans to train practitioners from all EU Member States in mutual legal assistance and cooperation in particular with the United States as the third country receiving the largest number of requests from the EU.[71] The EU also participates in the negotiations for the second additional protocol to the Budapest Convention, the main international instrument in cyber-crime.

Better co-ordination between external action and Justice and Home Affairs policies is crucial in the fight against cybercrimes. Greater coherence is needed not only among EU instruments, but also to coordinate the external activities of the individual Member States.[72] The next section will unveil how cyber threats can be handled through the CFSP.

## IV. Mainstreaming cybersecurity into the CFSP

The EU's development of collective responses to cyber-attacks has rested on a recognition that the multiplication of cyber-attacks and their destructive character required a different

[65] E Fahey, 'The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security' (2014) European Journal of Risk Regulation 46.

[66] G Butler and RA Wessel, 'Happy Birthday ERTA! 50 Years of the Implied External Powers Doctrine in EU Law' (31 March 2021) EU Law Blog www.europeanlawblog.eu.

[67] C Matera, 'Some Reflections on the Nature and Scope of the Externalisation of the AFSJ Domains' cit.

[68] Commission SWD(2018) 118 final cit.

[69] S Carrera and others, 'Access to Electronic Data by Third-Country Law Enforcement Authorities Challenges to EU Rule of Law and Fundamental Rights' (*Centre for European Policy Studies* 2015); J Daskal, 'Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues', (2016) Journal of National Security Law & Policy 473.

[70] T Christakis and F Terpan, 'EU–US Negotiations on Law Enforcement Access to Data: Divergences, Challenges and EU Law Procedures and Options' (2021) International Data Privacy Law 81.

[71] Proposal COM(2018) 225 final cit.

[72] European Security Strategy (2003) 15895/03.

response, beyond the conventional defence of networks and resilience-building paradigm. This called for a less inward-looking approach towards cyber-incidents and for a more outward-looking EU. In order to do this, the Union needed regulatory tools to address emerging hybrid threats to its security coming from the outside.

This *externalisation of EU cybersecurity* is a direct consequence of the institutional architecture that stems from the Lisbon Treaty that abolished the pillar structure. This led to an integration of the CFSP and other external objectives in single provisions and for a somewhat less fragmented decision-making process.[73] For instance, the 2013 cybersecurity strategy[74] was a product of a direct cooperation of three different bodies of the EU, with roots in the pre-Lisbon pillar-structure.[75] DG CONNECT (former pillar 1), the EEAS responsible for managing and developing the common foreign and security policy (former pillar 2) and DG HOME (previously pillar 3) adopted a holistic approach to cybersecurity by drawing different aspects into one structured document.[76] The involvement of the EEAS in the work on the 2013 Cybersecurity Strategy might be one of the reasons why this document elevates mainstreaming cybersecurity issues into EU external relations and Common Foreign and Security Policy as one of the EU's priorities.

The 2013 Cybersecurity Strategy is a steering document for the development of the EU Cyber Diplomacy Toolbox and EU's cyber defence. Cyber diplomacy and cyber defence emerge as the main aspects of the EU's cybersecurity under the CFSP. While they are inherently intertwined, they pursue different objectives. Cyber defence aims at protecting the EU against external threats by military and civilian means, whereas cyber diplomacy relies on non-military diplomatic means. Cyber diplomacy emphasises the need to work towards a coherent EU International cyberspace policy by improving coordination of global cyber issues and promoting EU values in cyberspace.[77]

### IV.1. The emergence of cyber cooperation under PESCO

Cyber defence is a key aspect of the Strategic Compass and of the EU Cybersecurity Strategy.[78] The special role of the Common Security and Defence Policy (CSDP) in addressing cyber threats has been articulated in the EU Cyber Defence Policy Framework

[73] RA Wessel, 'Integration and Constitutionalisation in EU Foreign and Security Policy, in R Schütze (ed), *Globalisation and Governance: International Problems, European Solutions* (CUP 2018) 339; RA Wessel, 'General Principles in EU Common Foreign and Security Policy' in V Morena-Lax, P Neuvonen and K Ziegler (eds), *Research Handbook on General Principles of EU Law* (Edward Elgar Publishing 2022) 606.

[74] The EU 2013 Cybersecurity Strategy cit.

[75] R Dewar, 'Cyber-Lisbon? The Impact of the Treaty of Lisbon on European Union Cybersecurity Policy' (2015) EUSA Conference Proceedings aei.pitt.edu.

[76] *Ibid.*

[77] The EU 2013 Cybersecurity Strategy cit.

[78] *Ibid.*; Council, 'A Strategic Compass for Security and Defence' 7371/22, 21 March 2022; Josep Borrel, *Cyber Defence: Speech on Behalf of High Representative/Vice-President Josep Borrell at the EP Plenary* www.eeas.europa.eu.

adopted in 2014 and updated in 2018.[79] The cooperation in the area of defence has always been marked by a differentiated approach across the EU,[80] and the cyber domain is no exception. Cyber elements of defence and security are included in the Permanent Structured Cooperation (PESCO) – launched in December 2017 – by 25 Member States. PESCO, established by art. 42(6) Treaty on European Union (TEU) and Protocol No. 10 to the Lisbon Treaty, has recently emerged as the most emblematic form of differentiated integration and enhanced cooperation in the EU.[81] It allows for small groups of Member States to work closely together in different areas of EU defence policy.

PESCO includes 10 cyber-related projects that aim at increasing efforts in the cooperation on cyber defence. The first set of PESCO cyber-related projects include: "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security" (CRRTs) and "Cyber Threats and Incident Response Information Sharing Platform".[82] CRRTs form part of a Lithuania-led force in operation since 2019. It was launched by Ministers of Defence of Croatia, Estonia, Poland, Lithuania, the Netherlands, and Romania. Belgium, Greece, Spain, Italy, France, Slovenia, and Finland have a status of observers. CRRTs operate by pooling participating Member States' experts and is equipped with unified Deployable Cyber Toolkits in order to detect and mitigate cyber threats.[83] It is on a permanent standby and can be activated to assist other Member States, EU Institutions, Common Security and Defence Policy (CSDP) operations as well as partners as soon as a concrete agreement on such assistance is reached. As an example, the EU's CRRTs was meant to be deployed to help Ukraine which has been facing cyber-attacks.[84] Lithuanian Deputy Defence Minister Margiris Abukevičius stressed that "It is important [...] to demonstrate solidarity with Ukraine and to provide it with assistance, and the deployment of the cyber rapid response team when needed is one of the objectives of the Lithuanian-led multinational project".[85] Nevertheless, this plan did not materialise due to the dramatic events that unfolded in the country after the start of the Russian war in Ukraine.

Another PESCO cyber-related project is the Strategic Command and Control (C2) System for CSDP missions and operations. Its objective is to enhance the military deci-

[79] Council, 'EU Cyber Defence Policy Framework' 15585/14, 18 November 2014; Council, 'EU Cyber Defence Policy Framework (2018 update)' 14413/18, 19 November 2018.

[80] B Leruth, S Gänzle and J Trondal, 'Differentiated Integration and Disintegration in the EU After Brexit: Risks Versus Opportunities' (2019) JComMarSt 1383.

[81] S Blockmans and DM Crosson, 'PESCO: A Force for Positive Integration in EU Defence'. (2021) European Foreign Affairs Review 87. Council Decision (CFSP) 2017/2315 of 11 December 2017 establishing permanent structured cooperation (PESCO) and determining the list of participating Member States.

[82] EU Cyber Defence Policy Framework (2018 update) cit.

[83] Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT) www.pesco.europa.eu.

[84] Lithuania may activate EU cyber force to help Ukraine' cit.

[85] *Ibid.*

sion-making process. More precisely it aims at the improvement of the planning and conduction of operations and missions, and the coordination of EU forces.

The practice of empowering the EU to deal with cybersecurity issues through the CFSP is reminiscent of the EU's fight against terrorism.[86] The Seville Declaration on the contribution of the CFSP to the fight against terrorism underlined the role of the CFSP and CSDP in countering terrorist threats to Union's security.[87] Along similar lines, the Declaration on combating terrorism adopted at the European Council in March 2004 underlined the role of the CFSP in the fight against terrorism.[88] This returned in the Treaty of Lisbon, which codified the special role of the CFSP and CSDP in fighting terrorism in art. 43 TEU, providing for the possibility to use civilian and military means in addressing terrorism. art. 43 TEU could be used by analogy to address cybersecurity related threats by joint Union operations and participation in common tasks, including through supporting third parties in their cyberspace stabilisation efforts. The support of third countries through confidence-building, preventive and restrictive measures is also foreseen in the EU Cyber Diplomacy Toolbox that will be analysed in the next section.

### IV.2. Cyber Diplomacy Toolbox: between sanctions and a lawful response to cyber-attacks

Faced with widespread cyber-attacks and a deadlock in the global negotiations on international law and state responsible behaviour in cyberspace,[89] the EU decided to develop its own framework for a joint EU diplomatic response to malicious cyber operations.[90] In 2016 the Dutch presidency submitted a Non-paper on "Developing a Joint EU Diplomatic Response Against Coercive Cyber Operations".[91] This document paved the way for the emergence of EU cyber diplomacy with a set of measures going beyond the traditional resilience and security of networks paradigm.

The *externalisation* of EU cybersecurity in order to deter and respond to cyber-attacks is in conformity with the CFSP objectives set out in art. 21 TEU. Accordingly, the Union's action on the international scene, inter alia, aims at "preserving peace, preventing conflicts and strengthening international security, in accordance with the purposes and prin-

[86] C Hillion, 'Fighting Terrorism Through the Common Foreign and Security Policy' in I Govaere and S Poli (eds) *EU Management of Global Emergencies* (Brill Nijhoff 2014).

[87] European Council, Declaration on the contribution of the ESDP in the fight against terrorism [2002].

[88] European Council, Declaration on combating terrorism [2004].

[89] F Delerue, 'International Cooperation on the International Law Applicable to Cyber Operations' (2019) European Foreign Affairs Review 203. The Group of governmental experts in the 2016–2017 UNGGE failed to reach a consensus in June 2017. Developments in 2021 were more positive: both the UNGGE and OEWG produced reports.

[90] Council Conclusions on cyber diplomacy cit.

[91] Council, 'Non-Paper: Developing a Joint EU Diplomatic Response Against Coercive Cyber Operations' 5797/6/16, 19 May 2016, www.statewatch.org.

ciples of the United Nations Charter, with the principles of the Helsinki Final Act and with the aims of the Charter of Paris".[92] While cybersecurity thus fits the Union's objectives, any action in that regard will also have to be guided by the mentioned principles.

In June 2017, the Council continued its work on the issue and presented its draft conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities.[93] Those conclusions refer to a range of diplomatic measures to be undertaken by the EU and Member States, including preventive measures, cooperative measures, stability measures and restrictive measures within the CFSP.

Preventive measures encompass EU-supported *Confidence Building Measures*, including initiatives in third countries through the European Neighbourhood Instrument (ENI) or any other relevant financing instruments. They also include awareness-raising on EU policies, such as EU-led political and thematic dialogues, particularly cyber or security dialogues.

Cooperative measures refer to EU-led political and thematic dialogues or EU-diplomatic *démarches* to facilitate the peaceful resolution of an ongoing incident.

Stability measures are understood as statements expressing concern or condemning general cyber trends[94] or cyber-attacks like *Wannacry* and *NotPetya* on behalf of the EU.[95] These include common positions by the Council, declarations by the High Representative of the EU,[96] EU Council Conclusions or démarches by the EU delegations as a way to signal the likely consequences of a malicious cyber activity.

Restrictive measures refer to sanctions under the CFSP that must, first, be proportionate to the scope, scale and duration of an aggressive behaviour in cyberspace.[97] Secondly, the use of restrictive measures is meant to deter potential perpetrators by influencing their rational cost-benefit analysis.

This paper devotes specific attention to two measures from the EU Cyber Diplomacy Toolbox. We will start with restrictive measures that were considered as a suitable foreign policy instrument for mitigating cyber threats and influencing the change of the behaviour of aggressors in the long term.[98] We will then reflect upon possibilities for EU support to Member States' lawful responses to cyber threats as foreseen under the Cyber Diplomacy Toolbox.

[92] Art. 21 TEU.

[93] Cyber Diplomacy Toolbox cit.

[94] Joint Statement by Presidents Tusk and Juncker and High Representative Mogherini on Russian Cyberattacks (4 October 2018) www.consilium.europa.eu.

[95] Council, Conclusions on malicious cyber activities 7925/18, 16 April 2018.

[96] In a declaration made on behalf of the Union on 12 April 2019, the High Representative urged actors to stop undertaking malicious cyber-activities that aim to undermine the Union's integrity, security and economic competiveness, including acts of cyber-enabled theft of intellectual property. Such cyber-enabled thefts include those carried out by the actor publicly known as "APT10" ("Advanced Persistent Threat 10").

[97] Council Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities cit. 4.

[98] Cyber Diplomacy Toolbox cit.

*a) Restrictive measures in response to cyber-attacks*

The European Union cyber sanctions framework is a new EU foreign policy tool that came into effect in May 2019.[99] It consists of two legal acts: Council Decision (CFSP) 2019/797 and Council Regulation (EU) 2019/796 providing for targeted restrictive measures against cyber-attacks threatening the Union or its Member States. The regular two-step procedure for adopting sanctions was followed. First, a CFSP decision[100] was adopted by the Council on the basis of art. 29 TEU laying down the overall sanctions framework. This was followed by the adoption of the associated Regulation[101] on the basis of art. 215 TFEU. Both legal acts are renewed every year.

Sanctions in response to cyber-attacks fall under the category of smart, unilateral sanctions. *Smart* in the sense that they adopt a targeted approach and are directed at the individuals and entities responsible for the attacks from a perspective of their conduct. These cyber-sanctions are different from the broad economic sanctions or sectoral economic sanctions that affect the entire population of a country by stalling the development of certain sectors of its economy. The EU cyber sanctions toolkit includes travel bans, asset freezes and prohibitions to make funds and economic resources available to those responsible for cyber-attacks. They thus constitute a personalised deterrence tool.

For the time being, eight natural persons and four entities or bodies are targeted by EU restrictive measures as being responsible for the attempted cyber-attack against the OPCW and the cyber-attacks publicly known as *WannaCry* and *NotPetya*, as well as *Operation Cloud Hopper*, and the cyber-attack on the German Federal Parliament (*Deutscher Bundestag*) in April and May 2015.[102] The EU has to date aligned itself to a large extent with the US cyber-related sanctions programme. For instance, in July 2020 it introduced

[99] For earlier assessment of cyber sanctions see Y Miadzvetskaya, 'Challenges of the Cyber Sanctions Regime Under the Common Foreign and Security Policy (CFSP)' in A Vedder and others (eds), *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security* (Intersentia, 2020) 277.

[100] Council Decision (CFSP) 2019/797 of 18 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

[101] Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

[102] Council Decision (CFSP) 2020/1127, cit.; Council Implementing Regulation (EU) 2020/1125 cit.; 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; 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; 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; Council Implementing Regulation (EU) 2020/1744 of 20 November 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

targeted sanctions against Russian, Chinese and North Korean entities and individuals that were already on the US cyber sanctions listings.[103]

The EU cyber sanctions framework is not country-specific but global in scope. Its main feature is indeed the shift to individual listings. Natural or legal persons are included on sanctions lists independently of a specific geographic area. This contrasts with most of the EU sanctions packages that are taken in response to major political crises and threats to peace and security in third countries (e.g. Belarus, Syria, Ukraine, Venezuela).

Cyber-attacks as the central focus of this sanctions regime are very distinct due to intrinsic features of cyberspace such as internet structural design and anonymity that constitute barriers to forensic-based technical attribution.[104] Cyber-attacks imply unauthorised actions that involve access to information systems, information system interference, data interference or interception.[105]

The EU cyber-sanctions framework is thus characterised by criteria for listing that are different from other sanctions regimes. These listing criteria refer to cyber-attacks that represent an external threat[106] and that have significant effects. The significance of an attack is assessed on the basis of the following criteria: scope, scale, impact or severity of disruption caused; number of natural or legal persons, entities or bodies affected; number of Member States concerned; the amount of economic loss caused; the economic benefit gained by the perpetrator; and the amount or nature of data stolen or accessed.[107] Sanctions may not just be imposed in case of successful attacks, but also in case of attempted attacks. As said by one EU official, the fact that a potentially harmful cyber-attack failed does not mean that it shall not be punished.[108]

The listing criteria in the cyber sanctions framework are, however, rather vague, which offers more flexibility to the Council, but also increases the likelihood of arbitrary decision-making. More precisely, the decision to include cyber-attack perpetrators or organisers on the EU sanctions lists is not only linked to them falling under specific listing criteria but also constitutes a political message. The lack of transparency with respect to sanctions designations is, however, a recurrent issue in EU sanctions practice and is not specific to the cyber sanctions framework.

The thematic nature of cyber sanctions also offers a higher degree of flexibility in contrast to country-specific measures. First of all, it allows the Council to act faster by updating the existing sanctions listings instead of enacting a completely new legal

[103] Y Miadzvetskaya, 'Cyber Sanctions: Towards a European Union Cyber Intelligence Service?' (College of Europe Policy Brief 1-2021).

[104] W Earl Boebert, 'A Survey of Challenges in Attribution' in National Academies, *Proceedings of a Workshop on Deterring Cyberattacks* (The National Academies Press 2010) 43.

[105] Council Decision (CFSP) 2019/797 cit. art. 1(3).

[106] *Ibid.* art. 1(2)(4).

[107] *Ibid*. art. 3.

[108] Interview with an EU official on file with the author.

framework each time a new sanction has to be imposed. Complex and lengthy procedures that are prone to Member State vetoes and which are typical for new country-specific designations are thus not required. Second, the personalised character better suits the present dynamics in the cyberspace in which states often rely on non-state actors – so-called proxies – to project their strategic interests.

Out of 46 sanctions regimes in place in the EU in 2022,[109] only four are horizontal and thematic in nature. Apart from cyber sanctions, these are sanctions addressing the use of chemical weapons, the EU's terrorist list, and the newly adopted Magnitsky-type Act against human rights abusers. The established cyber sanctions regime mirrors the EU framework on restrictive measures addressing the use and proliferation of chemical weapons.[110] The EU also contemplates thematic sanctions for spreading disinformation and undermining trust in democratic institutions. There are also some quasi-thematic sanctions regimes in place that pursue a specific objective while being tied to a particular country, for instance measures against Iran's nuclear program.[111]

*b) EU support to Member States' lawful responses*

In addition to the above-mentioned actions and instruments, the Treaties also foresee possibilities for EU support to or coordination of Member States' lawful responses to non-forcible and proportionate countermeasures to compel or convince an attacker to change their behaviour. After all, in grave instances, cyber-attacks could amount to a use of force or an armed attack within the meaning of art. 51 of the Charter of the United Nations. In this case, art. 42(7) TEU (the *Mutual Assistance Clause*) may be invoked by an attacked Member State to ask the EU and fellow Member States for aid and assistance. These collective defence arrangements are similar or even complementary to the collective defence provision in art. 5 of the North Atlantic Treaty.

In some other instances, the *solidarity clause* of art. 222 TFEU could be used for activating the help by other EU Member States.[112] The Treaty of Lisbon, for the first time in history, equipped the Union with a special provision aimed at improving the EU's solidarity in response to natural or man-made disasters. The *solidarity clause* creates an obligation for all Member States to act jointly "in a spirit of solidarity" and to assist one another in the event of disasters and crises which exceed their individual response capaci-

[109] For a complete overview of sanctions lists see www.sanctionsmap.eu.

[110] Council Decision (CFSP) 2018/1544 of 15 October 2018 concerning restrictive measures against the proliferation and use of chemical weapons.

[111] In addition to implementing UN sanctions, the EU imposed autonomous economic and financial restrictions on Iran. See for instance Council Decision 2010/413/CFSP of 26 July 2010 concerning restrictive measures against Iran and repealing Common Position 2007/140/CFSP.

[112] See for a recent overview of the options V Szép and others, 'The Current Legal Basis and Governance Structures of the EU's Defence Activities' (ENGAGE Working Paper Series 4–2021).

ties. Art. 222 TFEU stands in isolation from other Treaty provisions without being integrated in Union's external action provisions and without forming an inherent part of defence related treaty provisions.

The *solidarity clause* finds its roots in the Declaration on Solidarity Against Terrorism, issued by the European Council after the Madrid terrorist attacks in March 2004[113] and returned in the 2005 draft Constitutional Treaty that never entered into force. Initially two types of solidarity where contemplated by the Working group VIII on defence: solidarity in response to *armed aggression* and solidarity in the event of non-conventional threats.[114] It was believed that narrowing down the scope of solidarity to mutual defence arrangements could deprive the EU from the full range of its crisis and disaster management capacities.[115] Solidarity, set out in art. 222 TFEU, constitutes "a soft mutual defence commitment" covering non-conventional threats to the Union's security.[116] Such a broad solidarity approach, encompassing non-intentional disasters, also distinguishes the EU from a purely military alliance which was in particular relevant for some traditionally neutral Member States.[117]

Solidarity in the form of mutual assistance has contributed to shaping the EU's internal, external and security policies. Notably, mutual solidarity is referred to in arts 67(2) and 80 TFEU dealing with asylum, immigration and external border control as well as in art. 122 TFEU covering financial assistance in cases of severe difficulties caused by natural disasters or exceptional occurrences, and in art. 194 TFEU on EU energy policy.[118]

Contrary to the solidarity clause, the *Mutual Assistance Clause* in art. 42(7) TEU – which is quite similar to art. 5 of the NATO Treaty – remains a rather rhetorical concept without a defined implementing framework. Its activation imposes an obligation of aid and assistance on Member States, but does not seem to require any political coordination at the EU level. For the first time in history, the French Government officially invoked the *Mutual Assistance Clause* in the aftermath of the terrorist attacks in Paris on 13 November 2015.

The Treaty provisions do not make any explicit reference suggesting that the *solidarity clause* or *mutual assistance clause* may be invoked for cyber incidents. The type of events defined as covered by the *solidarity clause* include a terrorist attack and a natural or man-made disaster. "Disaster" in this context refers to any situation capable of se-

[113] Declaration on combating terrorism cit.

[114] S Blockmans, 'L'union fait la force: Making the Most of the Solidarity Clause (art. 222 TFEU)' in I Govaere and S Poli (eds) *EU Management of Global Emergencies : Legal Framework for Combating Threats and Crises* (Brill Nijhoff 2014) 111.

[115] *Ibid*., 113.

[116] T Konstadinides, 'Civil Protection in Europe and the Lisbon "Solidarity Clause": A Genuine Legal Concept or a Paper Exercise' (Uppsala Faculty of Law Working Paper 3-2011) 13.

[117] S Myrdal and M Rhinard, 'Empty Letter or Effective Tool' (UI Occasional Papers - The Swedish Institute of International Affairs 2/2010).

[118] T Konstadinides, 'Civil Protection in Europe' cit. 5.

verely impacting people, the environment or property, including cultural heritage.[119] This broad phrasing does, however, seem to offer enough flexibility to justify the activation of the *solidarity clause* in cases with a risk to a *severe impact*, which may encompass cyber-attacks affecting critical infrastructure or services necessary for the essential social activities, for instance in the sectors of energy or transport. As an illustration, a Distributed Denial of Service attack can result in severe impact on people by disturbing their access to public information or to the e-services provided. In the same vein, the recent cyber-attacks *WannaCry* and *NotPetya* displayed the disastrous paralysing effects that ransomware can have on the industry and society.

The relevance of a joint action and mutual assistance in a case of a major cyber incident or an attack was also confirmed in the EU Cybersecurity Strategy.[120] The latter explicitly states that a particularly serious cyber incident or attack could serve as a sufficient ground for a Member State to trigger the EU *solidarity clause*. The Council conclusions of November 2017 on cyber issues also highlighted that a particularly serious cyber incident or crisis could constitute sufficient ground to invoke the EU *solidarity clause* and/or the *mutual assistance clause*.[121]

There are diverging views on the temporal scope of the assistance foreseen under the *solidarity clause*. Some scholars believe that the emphasis is placed on the prevention and protection rather than on the actual assistance in dealing with consequences of a disaster.[122] At the same time, the European Parliament recalled in 2015 that art. 222 TFEU is specifically designed to deal with the consequences of the terrorist attacks in Europe.[123] The Cybersecurity Strategy similarly suggests that the solidarity clause deals with the consequences of an occurred incident, but cannot be activated on an *ex ante* basis for preventing a cyber-attack from occurring.[124] Consequently, any action under the auspices of EU solidarity is triggered in response to a disaster, upon request by a Member State. In other words, the *duty to prepare to assist* is a necessary first step anticipating the *duty to assist*.[125]

Hence, art. 222 TFEU can be relied upon in combination with some other Treaty provisions (including perhaps the principle of sincere cooperation under art. 4(3) TEU)[126] as a legal basis for adopting cybersecurity related legislation in the name of solidarity. However, it is not clear yet whether it can be used on its own to address certain

[119] Council Decision 2014/415/EU of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause.

[120] The EU 2013 Cybersecurity Strategy cit.

[121] Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 14435/17, 20 November 2017.

[122] T Konstadinides, 'Civil Protection in Europe' cit.

[123] European Parliament resolution of 21 January 2016 on the mutual defence clause (art. 42(7) TEU).

[124] The EU 2013 Cybersecurity Strategy, cit.

[125] S Blockmans, 'L'union fait la force' cit. 118.

[126] T Konstadinides, 'Civil Protection in Europe' cit p. 15.

threat scenarios. Some scholars held that it does not grant the EU a direct mandate to, for instance, develop defence policy instruments.[127] Instead, art. 222 TFEU would aim at strengthening the role of the EU in crisis management, such as the volcanic ash crisis of April 2010 and spread of pandemics like the H1N1 swine flu in April 2009 and Coronavirus in 2020.[128] The latter indeed put EU solidarity to the test.[129]

## V. The *externalisation* of the EU's cybersecurity and its limitations under CFSP

### V.1. The attribution of responsibility for cyber-attacks

The EU does not have procedures in place for the attribution of responsibility for cyber-attacks to third countries. Discussions on this topic are out of question at the moment since there is no political will to establish common attribution frameworks. Sanctions, mentioned in Cyber Diplomacy Toolbox, are targeted measures aimed at individuals, groups or companies and they do not lead to the attribution of responsibility to a State. While the guidelines of the Council of October 2017 initially referred to the possibility of the adoption of sanctions against a State when it carries out the malicious cyber activity or when it is deemed responsible for the actions of a non-state actor,[130] the May 2019 Council Decision emphasises the targeted nature of restrictive measures, excluding any attribution of responsibility for cyber-attacks to a third State.[131]

Nevertheless, Member States are free to make their own determinations with respect to the attribution of cyber-attacks. And contrary to some Member States, which publicly attributed cyber-attacks to specific States, the EU has not taken any act of attribution.[132] Moreover, any measure under the proposed Cyber Diplomacy Toolbox should take into account the broader context and objectives of the EU external rela-

[127] *Ibid*.

[128] *Ibid.*

[129] S Michalopoulos, 'Coronavirus Puts Europe's Solidarity to the Test' (6 March 2020) Euractiv www.euractiv.com.

[130] Council Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities cit. 5: "In the case where the malicious cyber activity is being carried out by a State, as well as in the case when a State is deemed responsible for the actions of a non-state actor that is acting under its direction or control, or if this State recognizes and adopts the behaviour of such a non-state actor as its own, the full range of measures in the Framework, including restrictive measures against that State, could be used by the EU and its Member States".

[131] Council Decision (CFSP) 2019/797 cit.; See also A. Bendiek and M. Schulze, 'Attribution: A Major Challenge for EU Cyber Sanctions' (SWP Research Paper 2021/RP 11).

[132] P Ivan, 'Responding to Cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox' (2019) European Policy Centre www.epc.eu.

tions, should be proportionate to malicious activities and should be based on a shared situational awareness agreed among the Member States.[133]

The targeted nature of cyber sanctions allows the EU to avoid the sensitive question of attribution of responsibility for cyber-attacks to a third country within the currently still underspecified international legal framework governing this area. Examples include the 2015 hack of the German Federal Parliament and the disrupting ransomware cyber-attacks (*WannaCry* and *NotPetya*), which paralysed the work of corporations and government agencies in 2017. As individual designations circumvent the establishment of State responsibility, the EU has *de facto* never attributed a cyber-attack to a third country, but has limited its actions to the expression of concerns and condemnations.

However, the delimitation between targeted measures and attribution of responsibility to a State remains rather superficial since a vast majority of cyber-attacks with high impact, such as the abovementioned *WannaCry* and *NotPetya*, were widely understood to have been orchestrated at the request and with the support of governments of, allegedly, North Korea and Russia respectively. 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. The EU has indeed attributed responsibility for cyber-attacks to individuals who worked for State bodies. As an example, the EU sanctioned four Russians including the current Head of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), while others work at different levels for the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU). Other sanctioned individuals and entities are connected to APT10 or APT38 known as a Chinese and North Korean state-sponsored threat groups that specialise in cyber operations.

### V.2. Evidence collection as a limitation for the EU Cyber Diplomacy Toolbox

Individual designations within the cyber-sanctions framework take place at three levels: legal, technical and political. Discussions first take place within the Horizontal Working Group on Cyber Issues, then in RELEX at the Council where political, legal and technical agreement is achieved and then finalised at COREPER. As the last step the Council adopts restrictive measures. Along this time designations have to be substantiated by evidence. Collecting evidence constitutes a sensitive issue which will be tackled in this section.

While sanctions in response to cyber-attacks constitute a novel personalised cyber deterrence tool, they are not immune to judicial review and must satisfy a set of procedural and substantive requirements. They must be accompanied by reasons for listings and sub-

[133] Cyber Diplomacy Toolbox cit.

stantiated with evidence.[134] Furthermore, this evidence must also be disclosed to the person listed in order to guarantee her defence and fair trial rights.[135]Taking into account that sanctions can be challenged in Court, the EU has to rely on evidence that the Council, more precisely Member States, will not be hesitant to share.[136] Most of EU sanctions listings now rely on open source data.[137] Such commitment to use open-source data for sanctions listings makes it easier to share those materials in Court. However, the main problem of data stemming from publicly available materials is their degree of reliability and accuracy.[138] The fact that they are in a public domain does not make them trustworthy, even more so when we speak about cyber and hybrid threats in our information was era.

This distinct feature makes the EU cyber sanctions system different from the one in the US on both ex-ante and ex-post levels. First, while the US cyber sanctions programme is more advanced and benefits from less fragmented decision-making, EU decision-making on sanctions still requires unanimity, even though a shift towards a qualified majority voting is contemplated.[139] Second, the US cyber-sanctions instrument is more flexible since the sanctions cannot be subject to appeal in the same manner as in the EU. While the EU's recent cyber sanctions framework provides for an extensive judicial review, questions remain with respect to evidence relating to each listed individual and entity. In our understanding, most of supporting evidence in question are of confidential nature. Data of such a sensitive nature would potentially hinder its disclosure in court.

Countering cyber threats indeed relies on an exchange of gathered intelligence which is not without difficulties due to a *sui generis* nature of the EU. The EU relies mostly on the cyber-related information provided by the EC3, EU Agency for Cybersecurity, EU's Computer Emergency Response Team (CERT-EU), and Member States, including their will to disclose such data, as well as the NATO. Taking into account the growing tendency towards the *externalisation* of the EU's cybersecurity, procedural and structur-

[134] Case C-417/11P *Council/Bamba* ECLI:EU:C:2012:718 para 49; Joined Cases T-307/12 and T-408/13 *Mayaleh v Council* ECLI:EU:T:2014:926 para 85; art. 296 TFEU provides that EU legal acts must state the reasons on which they are based.

[135] Joined Cases C-584/10 P, C-593/10 P and C-595/10 P *European Commission and Others v Yassin Abdullah Kadi* ECLI:EU:C:2013:518 para 130; See also C Eckes, 'EU Restrictive Measures Against Natural and Legal Persons: From Counterterrorist to Third Country Sanctions' (2014) CMLRev 869-905.

[136] Case T-228/02 *Organisation des Modjahedines du peuple d'Iran v. Council and UK (PMOI I)* ECLI:EU:T:2006:384 para 155; Joined Cases C-402/05 P and C-415/05 *P Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities* ECLI:EU:C:2008:461 paras 342-344; V Abazi and C Eckes, 'Closed Evidence in EU Courts: Security, Secrets and Access to Justice' (2018) CMLRev 753.

[137] C Eckes, 'EU Global Human Rights Sanctions Regime: Is the Genie Out of the Bottle?' (2021) Journal of Contemporary European Studies 255.

[138] *Ibid.* 265-266.

[139] European Parliament Resolution of 9 June 2022 on the Call for a Convention for the Revision of the Treaties para 6; See also K Pomorska and RA Wessel, 'Qualified Majority Voting in CFSP: A Solution to the Wrong Problem?' (2021) European Foreign Affairs Review 351.

al reforms might be needed, including in the framework of the CFSP, in order to enhance information sharing among Member States and stimulate cooperation with the private sector. In fact, as recent research reveals, the intelligence cooperation within the European Union is still very much in development and largely takes place behind closed doors.[140] Enhancing cooperation might be even more pressing taking into account that with Brexit the analysis provided by the British experts will be lost.[141]

Three avenues for enhancing the exchange of evidence could be contemplated in the EU. First, by using the possibilities offered by the PESCO. In this respect, the project Cyber and Information Domain (CID) Coordination Center (CIDCC) could serve as an example. It is meant to establish and operate a multinational Cyber and Information Domain (CID) Coordination Center (CIDCC). On the basis of the CIDCC, the participating Member States second their national staff, but decide on case-by-case basis for which threat, incident and operation they provide support.[142] Similar PESCO frameworks could provide a framework for cooperation between the willing.

A second road is through an enhanced cooperation on the basis of art. 329(2) TFEU that provides for the possibility to embark on the path of closer cooperation in the field of the CFSP. It foresees the possibility to start an enhanced cooperation among Member States in the CFSP provided it is authorised by the Council and is consistent with the CFSP and other Union policies.

A third and novel avenue involves cooperation with private parties. Given that the essential part of infrastructures are owned by private companies, their participation in threat analysis is crucial for the European and national security. The multi-stakeholder model for cybersecurity, including regular and structured exchanges with the private sector, was stressed in the EU Council Conclusions on EU's Cybersecurity Strategy for the Digital Decade[143] and the 2020 Cybersecurity Strategy.[144] In this respect, Microsoft constitutes an interesting example of a private entity sharing threat analysis data with EU institutions and advancing debates on EU cybersecurity through *European Cyber Agora* forum. Nevertheless, a steadily growing role of private companies in sensitive security-related issues raises questions with respect to the privatisation of public policies by a few stakeholders. Such a dynamic may lead to the equation of their status to that of public bodies that is not met with enthusiasm by everyone in Brussels and national capitals.

[140] V Szép, E Sabatino and RA Wessel, 'Developing Assessment Criteria for Security and Intelligence Cooperation in the EU' (ENGAGE Working Paper Series 2022).

[141] R Bossong, 'Intelligence Support for EU Security Policy' (SWP Comment 51-2018).

[142] European Parliament Resolution of 13 June 2018 on cyber defence.

[143] Commission, The EU's Cybersecurity Strategy for the Digital Decade (2020) JOIN(2020) 18 final.

[144] Council, Draft Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade, 6722/21, 9 March 2021.

## VI. Concluding remarks

The main aim of this *Article* was to assess the legal tools the European Union has in dealing with cyber-attacks. EU cybersecurity policies are still in their infancy. Yet, over the past two decades a number of instruments have been developed that directly or indirectly address cybersecurity concerns. As in most policy areas, this development started by extending internal rules on, for instance, the internal market and the Area of Freedom, Security and Justice to allow for cybersecurity dimensions to be taken into account. This was followed by what we have termed the *externalisation* of the EU's cybersecurity regime.

The increasing number of threats coming from (individuals in) third countries called for the Union to mainstream cybersecurity in its foreign and security policy. Just as with regard to internal measures, 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). This gradually led to a formulation of the Union's cyber diplomacy in 2015, followed by a Cyber Diplomacy Toolbox in 2017 that was subsequently filled to allow the Union to react in a more comprehensive manner to the increasing number of threats that form a serious risk to essential infrastructures in the Member States as well as to the Union's own institutions.

Despite the many instruments that have been adopted, the Union continues to face a number of challenges. One of them is the absence of attribution procedures at the EU level. This omission significantly hinders common action by the EU Member States and leaves this prerogative in the realm of national decision-makers. Since the attribution of responsibility lays at the core of sovereign powers of Member States, there is no political will to transfer those prerogatives to the EU level at the moment. Assuming that such transfer takes place in the future, the operationalisation of common attribution procedures may be subject to disagreements between Member States compounded by uneven cyber-capabilities.

The second challenge relates to the evidence collection in the EU that still relies on data collected by national experts. Access to evidence is essential for the EU's situational awareness. The EU Cyber Diplomacy Toolbox will be significantly strengthened if information exchange gets reinforced under PESCO programs or through an enhanced cooperation on the basis of art. 329(2) TFEU that provides for the possibility to embark on the path of closer cooperation in the field of the CFSP. The multi-stakeholder model for cybersecurity, including regular and structured exchanges with the private sector is another avenue for improving cyber threat information sharing in the EU.

Overall, while an indirect use of legal bases has allowed the Union to adopt an impressive set of internal instruments to deal with cybersecurity, the step to *externalise* these instruments and use them in relation to external action is still at a first stage, despite the gradual mainstreaming of cybersecurity in the Union's foreign and security policy. The current war in Ukraine, and the cyber threats that come with it, may however speed-up the process in the direction of a true cyber diplomacy coordinated by the European Union.