Defending the security of the EU constitutional order against malicious cyber activity: Reflections on the cyber targeted sanctions regime

Susanna Villani[*]

1. *Introduction*

The magnitude, frequency, and impact of cyber incidents and attacks for the purposes of cyberespionage, ransomware, disruption, and destabilisation are increasing on a global scale. In addition to jeopardising the effective operation of network and information systems, these threats have the potential to erode the capacity to safeguard essential economic interests, maintain public order, and, in general, uphold national and supranational security.[1]

In this context, the European Union (EU) has gradually developed a complex and evolving legal framework aimed at managing cybersecurity issues, although national security remains an exclusive responsibility of the Member States pursuant to Article 4(2) TEU.[2] In 2013, the first strategy was adopted by the European Commission with the Communication

[*] Junior Assistant Professor in EU Law at the Department of Legal Studies of the University of Bologna.

[1] For insights, see K Kittichaisaree, *Public International Law of Cyberspace* (Springer 2017); N Tsagourias, R Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar 2021); H Lahmann, *Unilateral Remedies to Cyber Operations* (CUP 2020); AL Sciacovelli, 'Malicious Cyber Operations Committed by States and Non-State Actors: The International Legal Landscape', in P Gargiulo, D Giovannelli, AL Sciacovelli (eds), *Cybersecurity Governance and Normative Frameworks: Non-Western Countries and International Organizations Perspectives* (Editoriale Scientifica 2024) 7-33.

[2] For comments, see, among the others, E Cloots, *National Identity in EU Law* (OUP 2015); L Corrias, 'National Identity and European Integration: the Unbearable Lightness of Legal Traditions' (2016) Eur Papers 383-393; G Di Federico, *L'identità nazionale degli Stati membri nel Diritto dell'Unione Europea. Natura e portata dell'art. 4, par. 2, TUE* (Editoriale Scientifica 2017).

on *An Open, Safe and Secure Cyberspace*,[3] which included the following strategic priorities: (1) achieving cyber resilience; (2) drastically reducing cybercrime; (3) developing cyber-defence policy and capabilities related to the Common Security and Defence Policy (CSDP); (4) developing the industrial and technological resources for cybersecurity; and (5) establish a coherent international cyberspace policy. And effectively, cybersecurity has been integrated transversally within multiple EU policies in order to build resilience, fight cybercrime, support cyber defence, and develop industrial and technical resources for cyberspace.[4]

The 2020 Joint Communication on the *EU Cybersecurity Strategy for the Digital Decade* triggered the adoption of new regulatory, policy and investment instruments to ensure that everyone can 'lead a secure digital life' and create 'a resilient Europe, green and digital'.[5] In addition to considerations pertaining to the internal market, the document underlined the necessity to further develop a *EU External Cyber Capacity Building*

[3] European Commission, *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN/2013/01 final.

[4] In this regard, see European Commission and High Representative, *Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU* (13 September 2017) JOIN/2017/0450 final. For comments, see E Fahey, 'The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security' (2014) 5 European J Risk Regulation 46-60; G Christou, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy* (Palgrave MacMillan 2016); H Carrapico, A Barrinha, 'European Union Cyber Security as an Emerging Research and Policy Field' (2018) 19 Eur Politics and Society 299-303; G Gonzalez Fuster, L Jasmontaite, 'Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights', in M Christen, B Gordijn, M Loi, (eds), *The Ethics of Cybersecurity, The international Library of Ethics, Law and Technology* (Springer 2020) 109.

[5] European Commission, *Joint Communication to the European Parliament and the Council: The EU Cybersecurity Strategy for the Digital Decade* (16 December 2020) JOIN/2020/18 final. For comments, see J Odermatt, 'The European Union as a Cybersecurity Actor' in S Blockmans, P Koutrakos (eds), *Research Handbook on EU Common Foreign and Security Policy* (Edward Elgar 2018) 359; AP Brandão, I Camisão, 'Playing the Market Card: The Commission's Strategy to Shape EU Cybersecurity Policy' (2022) 60 J Common Market Studies 1335-1355.

Agenda to steer efforts in the field of digitalisation where to include cybersecurity as a standard feature of the EU external action.[6] Indeed, cybersecurity represents a specific component of the supranational strategy for 'an effective and genuine Security Union'[7] against exogenous influences that could undermine the EU constitutional order and construction of a (self-proclaimed) sovereignty[8] also in the digital dimension.[9] This perspective operates in conjunction with the so-called 'EU technological (or digital) sovereignty',[10] combined with the notion of 'strategic autonomy'.[11] In brief, the combination of these concepts reflects the Union's

[6] *The EU Cybersecurity Strategy for the Digital Decade* (n 5) point 3.3. To be noted that the Council had already adopted conclusions on *EU External Cyber Capacity Building Guidelines* on 26 June 2018.

[7] European Commission, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy* (24 July 2020) COM/2020/605 final. More recently, see European Council, *Strategic Agenda 2024-2029* available at <www.consilium.europa.eu/media/4aldqfl2/2024_557_new-strategic-agenda.pdf>.

[8] On the emerging broader concept of 'European sovereignty', see S Barbou des Places, 'Taking the Language of "European Sovereignty" Seriously' (2020) 5 Eur Papers 287-297.

[9] R Wessel, 'European Law and Cyberspace', in N Tsagourias, R Buchan (eds) *Research Handbook on International Law and Cyberspace* (Edward Elgar 2021) 490-507.

[10] Starting with the 2020 State of the Union, references to 'technological or digital sovereignty' are numerous: European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Shaping Europe's digital future* (19 February 2020) COM/2020/67 final; A New Industrial Strategy for Europe (10 March 2020) COM/2020/102 final, *Industrial Strategy 2020 Update: Building a Stronger Single Market for Europe's Recovery* (5 May 2021) COM/2021/350 final.

[11] For comments, see Editorial Comments, 'Keeping Europeanism at Bay? Strategic Autonomy as a Constitutional Problem' (2022) Common Market L Rev 313; N Helwig, V Sinkkonen, 'Strategic Autonomy and the EU as a Global Actor: The Evolution, Debate and Theory of a Contested Term' (2022) 27 Eur Foreign Affairs Rev 1-20; S Poli, E Fahey, 'The Strengthening of the European Technological Sovereignty and Its Legal Bases in the Treaties' (2022) Eurojus.it 147-164; G De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (CUP 2022); F Hoffmeister, 'Strategic Autonomy in the European Union's External Relations Law' (2023) 60 Common Market L Rev 667-670; E Kassoti, R A Wessel, 'Strategic Autonomy: The Legal Contours of a Security Policy Construct' (2023) 28 Eur Foreign Affairs Rev 305-310; C Rapoport, 'Setting Norms and Promoting a Rules-based International Legal Order: Enhancing Strategic Autonomy Through the Autonomy of the EU Order' (2023) 8 Eur Papers 447-457; S Poli, D Gallo, 'Enhancing European Technological Sovereignty: The Foreign Investment Screening Regulation and Beyond', in KA Armstrong, J Scott, A

intention to overcome its dependence on foreign subjects and to contribute to the shaping of international rules also in the digital/technological domain. This should also allow the EU to protect its identity based upon the values set in Article 2 TEU,[12] while promoting abroad its own standards, principles, and (exactly) values according to Articles 3(5) and 21(1) TEU.[13] In fact, the primary objective of the EU's external action is to protect its 'values, fundamental interests, security, independence and integrity', as explicitly stated in Article 21(2)(a) TEU.

Building on these theoretical premises, this work aims to examine recent developments in the Union's cybersecurity instruments under the Common Foreign and Security Policy (CFSP) from a constitutional perspective, taking into account the EU's value-based legal framework. In particular, the analysis focuses on the adoption of restrictive measures against cyber malicious activities from abroad as an instrument of CFSP to counter this type of threat.[14] As a matter of fact, targeted restrictive

Thies (eds), *EU External Relations and the Power of Law: Essays in Honour of Marise Cremona* (OUP 2024) 215-250.

[12] The contours of the EU constitutional identity, based on the values referred to in art 2 TEU as already identified in Opinion 2/13 on the EU's accession to the European Convention on Human Rights, emerged clearly in the judgments rendered by the Court of Justice in February 2022 (Case C-156/21 *Hungary v Parliament and Council* [2022] ECLI:EU:C:2022:97, Case C-157/21 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:98). For comments, PS Pohjankoski, 'The Unveiling of EU's Constitutional Identity - Judgments in C-156/21, Hungary v. Parliament and Council and C-157/21, Poland v. Parliament and Council' (2022) *EU Law Live – Weekend Edition*; A Festa, 'The "twin" judgments of 16 February 2022: beyond the question of legitimacy, a "manifesto" on the foundations of European law' (2022) Papers of Eur L 81-110; G Contaldi, 'Le sentenze della Corte di giustizia sui ricorsi di Polonia e Ungheria e l'emersione del concetto di identità europea' in G Contaldi, R Cisotta (eds), *Courts, Values and European Identity* (Eurojus 2022) 87-103; LS Rossi, '"Concretised", "Flanked", or "Standalone"? Some Reflections on the Application of Article 2 TEU' (2025) 10 Eur Papers 1-24.

[13] See, *inter alia*, M Cremona, 'Values in EU Foreign Policy', in M Evans, P Koutrakos (eds), *Beyond the Established Orders: Policy Interconnections between the EU and the Rest of the World* (OUP 2011) 275-315; L Mola, 'Fostering 'European Technological Sovereignty' Through the CSDP: Conceptual and Legal Challenges. First Reflections Around the 2022 Strategic Compass' (2023) 8 Eur Papers 459-474.

[14] In EU law, 'sanctions' are also called 'restrictive measures'; therefore, this paper uses them synonymously. For insights, F Casolari, 'EU Sanctions Policy: A Legal Appraisal in Light of the EU's Strategic Autonomy Doctrine', in G Adinolfi, A Lang, C Ragni (eds), *Sanctions By and Against International Organizations* (Intersentia 2024) 29. About the EU sanctions regime, see, *inter alia*, F Costamagna, A Miglio, S Montaldo (eds), *EU Law Enforcement. The Evolution of Sanctions Powers* (Routledge 2020); K

measures potentially serve a dual function in constitutional terms. In the first place, they may represent a reactive mechanism aimed at protecting the EU constitutional order, by imposing tangible consequences on individuals, entities, and bodies responsible for malicious cyber activities. In the second place, they may contribute to the external projection of EU founding values, reaffirming the Union's commitment to the rule of law, the protection of fundamental rights, and the defence of democratic systems in cyberspace. Based on the idea that 'our security is linked to our fundamental values',[15] the adoption of restrictive measures shall thus be instrumental not only in ensuring the effective functioning of the EU internal market but also in protecting the integrity and security of the Union, its Member States and their citizens against cyber threats and malicious cyber activities.

The article is structured as follows. First, it provides an overview of the EU's external cyber strategy, focusing on the main legal instruments related to cyber defence and cyber diplomacy under the CFSP (Section 2). The analysis then turns to the recent practice of adopting targeted restrictive measures against malicious cyber activities as a 'reactive tool' of the EU's cyber diplomacy strategy (Section 3). Based on the challenges that characterise this system of sanctions, the article will critically assess the consistency with the EU's constitutional constraints and its effective contribution to the Union's security (Section 4). Finally, it offers some conclusive reflections (Section 5).

2. *The EU external strategy on cybersecurity: Between cyber defence and cyber diplomacy*

The EU's Common Foreign and Security Policy does not explicitly address cybersecurity, but, under Article 24(1) TEU, the 'Union's competence in matters of common foreign and security policy shall cover all areas of foreign policy and *all questions relating to the Union's security*' (emphasis added). Upon these premises, the EU has progressively framed cybersecurity issues within the broader CFSP; an expansion that has

Urbanski, *The European Union and International Sanctions: A Model of Emerging Actorness* (Edward Elgar 2020).

[15] *EU Security Union Strategy* (n 7) point V.

raised questions about the scope and limits of EU competence in the absence of a dedicated legal basis for cyberspace governance, thereby exposing overlaps between supranational and intergovernmental instruments in the external domain.[16]

In 2020, the Commission adopted the Communication *Shaping Europe's Digital Future*[17] and, shortly afterwards, the new *Security Union Strategy* for the period 2020-2025,[18] setting out further tools and measures to be developed to ensure the security of both the physical and digital environment. The elements of attention ranged here from the fight against terrorism to organized crime, passing through the prevention and detection of hybrid threats and the increase in the resilience of critical infrastructures, up to the strengthening of cybersecurity and the promotion of research and innovation.

As set out in *The Strategic Compass for Security and Defence* approved by the Council in March 2022,[19] the conflict between Russia and Ukraine has then reinforced the need to revise the supranational defence strategy in the cyber domain. Here it was affirmed that 'the EU urgently needs to take more responsibility for its own security by acting in its neighbourhood and beyond, with partners whenever possible and alone when necessary'.[20] Thus, following the Council's recommendation on the development of the Union's position on cyber deterrence, in November of the same year the High Representative and the Commission jointly presented the Communication on *The EU's Cyber Defence Policy*.[21] It entails the enhancement of instruments for defence cooperation and collaboration between States, the improvement of collective situational awareness and early detection capacity, and the provision of the EU with adequate cyber skills capable of developing and managing digital technologies. On 23 May 2023, the Council adopted conclusions on the *EU policy on cyber*

[16] L Pupillo, MK Griffith, S Blockmans, A Renda, '*Strenghtening the EU's Cyber Defence Capabilities*' (*CEPS*, 26 November 2018) available at <www.ceps.eu/ceps-publications/strengthening-eus-cyber-defence-capabilities/>.

[17] *Shaping Europe's digital future* (n 10).

[18] *EU Security Union Strategy* (n 7).

[19] Council Document 7371/22 of 21 March 2022, *A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security*.

[20] ibid point 23.

[21] European Commission, *Joint Communication to the European Parliament and the Council: EU Policy on Cyber Defence* (10 November 2022) JOIN/2022/49 final.

defence, stressing the importance of further strengthening the EU's resilience in order to face up to cyber threats.[22]

Based on these orientations, the actions and instruments that have been progressively adopted as part of the CFSP have tended to be more varied in nature. They can be divided into two distinct categories, which, although inherently interlinked, are characterised by a different degree of EU intervention due to its intrinsic limitation in the defence domain.

The first category concerns proper cyber defence initiatives to protect Member States against external threats through greater cooperation and synergies between military and civilian networks' capacities. Major activities in the military field have been carried out by the Permanent Structured Cooperation (PESCO), that is the most emblematic form of differentiated integration and enhanced cooperation in the EU established under Article 46(2) TEU and Protocol 10 to the Lisbon Treaty.[23] Through the Cyber Rapid Response Teams (CRRTs) and Mutual Assistance in Cyber Security, and the Incident Response Information Sharing Platform, military capabilities intervene in particular with regard to the identification of hybrid threats, an area requiring progress due to the current insufficient level of strategic guidance and different maturity levels of Member States. However, it should be noted that adherence to PESCO is at the discretion of Member States, thus not being capable to fill the gaps in harmonisation, while rising questions on the effective coordination with the NATO cyber capabilities[24] and highlighting the structural limitations of a voluntary framework in fostering harmonised and binding EU-wide cyber defence standards.

Outside of PESCO, cyber defence tools focus on developing training and defensive exercises also within the European Defence Agency to address cybersecurity skills gaps. The investments on cybersecurity are sup-

[22] Council Document 9618/23 of 22 May 2023, *Council Conclusions on the EU Policy on Cyber Defence*.

[23] Council Decision (CFSP) 2017/2315 of 11 December 2017 establishing permanent structured cooperation (PESCO) and determining the list of participating Member States [2017] OJ L 331. For insights, see S Blockmans, DM Crosson, 'PESCO: A Force for Positive Integration in EU Defence' (2021) Eur Foreign Affairs Rev 87-110; L Lonardo, *EU Common Foreign and Security Policy After Lisbon* (Springer 2023).

[24] NATO and the EU signed a Technical Arrangement on Cyber Defence in February 2016 between NATO's Computer Incident Response Capability and the EU's Computer Emergency Response Team.

ported by the European Defence Fund that supports collaborative projects fostering research and industrial development of capabilities.[25] In any case, as recently stressed in the *White paper for European defence – Readiness 2030*, [26] these are activities imagined and conducted to strengthen the (voluntary) management and response capacities of Member States, considered that they have the operational capabilities and the primary responsibility in the management of cyber crises. The Union's current role in cyber defence remains primarily that of a facilitator and coordinator, rather than a centralised actor with autonomous operational capacity.

As a result, the EU's ability to respond to large-scale cyber incidents hinges on the collective political will and preparedness of Member States – particularly in the absence of binding obligations or integrated command structures. This scenario, which puts Member States at the centre, also recalls the Mutual Defence Clause set out in Article 42(7) TEU[27] which obliges (just) the Member States to provide 'aid and assistance by all the means in their power' in case of armed aggression and that could be potentially invoked in the context of a serious cyber-attack that constitutes an armed aggression; an eventuality that remains uncertain both in legal and practical terms. Thus, while the EU's cyber initiatives may contribute to a shared baseline of resilience and readiness, they do not amount to a collective defence mechanism in themselves; rather, they

[25] The Commission adopted the European Defence Fund's annual Work Programme for 2025, allocating €1,065 billion for collaborative research and development in the field of defence. It supports the development of critical defence technologies and capabilities in all military domains, including ground, air, naval, space, and cyber in line with the EU capability priorities agreed by Member States.

[26] European Commission, *Joint White Paper for European Defence Readiness 2030* (28 March 2025) JOIN/2025/120 final.

[27] For insights, F Delerue, 'The Threshold of Cyber Warfare: from Use of Cyber Force to Cyber Armed Attack', in *Cyber Operations and International Law* (CUP 2020) 273; I Kilovaty 'Cyber Conflict and the Thresholds of War', in DL Sloss (ed), *Is the International Legal Order Unraveling?* (OUP 2022) 251–282. For insights on the clause, see T Ramopoulos 'Article 42 TEU', in M Kellerbauer, M Klamert, J Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (OUP 2019) 276; HB Hosang, P Ducheine, 'Implementing Article 42(7) of the Treaty on European Union: Legal Foundations for Mutual Defence in the Face of Modern Threats' in S Marquardt, S Blockmans (eds), *The European Union's Contribution to International Peace and Security* (Brill 2023) 214-242.

serve to prepare the ground for a coordinated response should such a threshold ever be reached.

The second group of instruments belongs to cyber diplomacy, which essentially relies on diplomatic measures to work towards a coherent EU international stance by improving coordination of global cyber issues and promoting EU founding values in cyberspace. It is comprised under the umbrella of the *Joint EU Diplomatic Response on Malicious Cyber Activities*, also known as '*Cyber Diplomatic Toolbox'*, adopted by the Council in 2017.[28] The 2020 *EU Cybersecurity Strategy* has then reinforced the EU's diplomatic response to cyberattacks, by requiring the adoption of implementing guidelines in order to create a solid linkage with the EU crisis management ecosystem.[29] For that, in comparison to the cyber defence instruments, the diplomatic initiatives are oriented to promote the active engagement of the EU as a whole rather than as a simple hub of cooperation for the Member States.

The measures comprised in the *Cyber Diplomacy Toolbox* have political, legal, strategic, technical, operational or economic nature, focusing on the delivery of preventive, stabilising, cooperative, normative, restrictive, supportive or mitigative effects thus enhancing the Union's assertive stance worldwide.[30] In particular, the toolbox requires efforts to adhere to the peaceful settlement of international disputes in cyberspace and the commitment to actively support the development of voluntary, non-binding norms of responsible State behaviour drawn from the reports issued by the UN GGE.[31] Coherently, the toolbox includes formal 'cyber dia-

[28] Council Document 10474/17 of 19 June 2017, *Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox')*. For comments, see Y Miadzvetskaya, RA Wessel, 'The Externalisation of EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox' (2022) 7 Eur Papers 413-438.

[29] *The EU Cybersecurity Strategy for the Digital Decade* (n 5). Then, the Council adopted the *Revised Implementing Guidelines of the Cyber Diplomacy Toolbox* (Council Document 10289/23 of 8 June 2023) point 6.

[30] A Bendiek, 'The EU as a force for peace in international cyber diplomacy' (*SWP*, 26 April 2018) available at <www.swp-berlin.org/publikation/the-eu-as-a-force-for-peace-in-international-cyber-diplomacy>.

[31] 'Report of the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the context of international security' UN Doc A/70/174 (22 July 2015); 'Report of the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the context of international security' UN Doc A/68/98 (24 June 2013). For an alignment of EU law with

logues' on technical and market-related issues in the form of bilateral relations with strategic partners (US, Japan, India, South Korea, China).[32] In addition, the *Toolbox* envisages the establishment of an informal *Cyber Diplomacy Network* and a structured exchange with regional organisations such as the African Union, the ASEAN Regional Forum, the Organisation of American States and the Organisation for Security Cooperation in Europe. Such a commitment has been recently confirmed in the Communication on the *European Preparedness Union Strategy*, which has underlined the necessity of a close coordination with NATO and other like-minded partners to dissuade threat actors as well as to build mutual resilience and preparedness.[33] This seems to be aligned with Articles 21(1) TEU and 220 TFEU, which require the Union to promote multilateralism as an approach to common problems by developing relations and establishing partnerships with third countries and international, regional or global organisations.[34] From a strategic point of view, the choice to rely on soft law instruments and market-oriented solutions reflects the current Union's orientation to pursue a promotional, rather than assertive, strategy in advancing in the cyber domain through a flexible and cooperative model. Yet, the effectiveness and legal robustness of such measures remain dependent on politically sensitive assessments of attribution and proportionality, often without clearly established procedural safeguards or judicial oversight mechanisms.

Besides such a preventive and cooperative approach, the *Cyber Diplomacy Toolbox* deals with the reaction to malicious cyber activities, by suggesting to use the full range of instruments available at EU level, such as

international law on cybersecurity issues, see Council Document 15833/24 of 18 November 2024, *Council Declaration on a Common Understanding of International Law in Cyberspace*.

[32] T Renard, 'EU Cyber Partnerships: Assessing the EU strategic partnerships with third countries in the Cyber Domain' (2018) 19 Eur Politics and Society 321.

[33] European Commission, European Commission, *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Preparedness Union Strategy* (26 March 2025) JOIN/2025/130 final, points 5 and 7.

[34] For insights, E Neframi, 'The Dynamic of the EU Objectives in the Analysis of the External Competence', in E Neframi, M Gatti (eds), *Constitutional Issues of EU External Relations Law* (Nomos 2018) 63-88.

the adoption of targeted restrictive measures.[35] In this regard, the Council set a list of six guiding principles ranging from the final goal of these measures under Article 21(2)(a) TEU ('to protect the integrity and security of the EU, its Member States and their citizens') to the nature of the measures ('be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity') and to the general constraints ('respect applicable international law and not violate fundamental rights and freedoms').[36]

3. *The EU targeted restrictive measures regime against malicious cyber activities*

On the basis of Article 29 TEU, which empowers the Council to decide about the Union's approach to a particular matter of a geographical or thematic nature, the EU can adopt autonomous and unilateral restrictive measures.[37] The decisions adopted by unanimity under Article 31(1) TEU[38] shall be then implemented by means of a Council Regulation adopted by a qualified majority on the basis of Article 215(2) TFEU, and further accompanied by explanatory notes adopted in the guise of Council implementing regulations.[39] As well known, sanctions on individuals

[35] For a comment upon sanctions as instrument of coercive diplomacy, see N Ronzitti, 'Sanctions as Instruments of Coercive Diplomacy: An International Law Perspective', in N Ronzitti (ed), *Coercive Diplomacy, Sanctions and International Law* (Brill/Nijhoff 2016) 1-32.

[36] *Cyber Diplomacy Toolbox* (n 28) point 5.

[37] For insights, see C Beaucillon, *Les mesures restrictives de l'Union européenne* (Bruylant 2014); L Borlini, S Silingardi, 'Defining Elements and Emerging Legal Issues of EU Sanctions' (2018) Italian YB Intl L 33-52; S Poli, *Le misure restrittive autonome dell'Unione Europea* (Editoriale Scientifica 2019); T Ramopoulos, 'Article 29 TEU', in M Kellerbauer, M Klamert, J Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (OUP 2019) 236-239.

[38] R Bottner, RA Wessel, 'Article 31 [Procedures for the Adoption of CFSP Decisions]', in HJ Blanke, S Mangiameli (eds), *The Treaty on European Union (TEU): A Commentary* (Springer 2013) 1058.

[39] F Erlbacher, 'Article 215 TFEU', in M Kellerbauer, M Klamert, J Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (OUP 2019) 1631-1641.

and entities are subject to periodic review and theoretically to scrutiny by the Court of Justice under Article 275 TFEU.[40]

The legal framework for targeted restrictive measures against cyber attacks was introduced in May 2019, with the adoption of Council Decision (CFSP) 2019/797[41]and Council Regulation (EU) 2019/796.[42] In relation to the scope *ratione personae*, measures can be taken against actors directly responsible for cyber attacks, as well as those involved in, or providing financial, technical or material support to, a cyber-attack. The measures consist of the classical prohibitions on entry (generally called travel bans or visa bans) and asset freezes, both of which are applied via lists of designated individuals and entities featured in the annex. It is worth noting that the effectiveness of these measures may be questioned in light of the distinctive nature of cyber threats. Travel bans and asset freezes often have limited deterrent power when targeting State-affiliated actors, individuals shielded from international exposure, or those operating through anonymous or proxy networks. Hence, although symbolically significant and norm-setting in intent, such sanctions may fail to materially weaken the operational capability of the threat actor. This limitation is further compounded by the distinctive features of cyberspace, which make cyber-attacks a particularly complex focus for the sanctioning regime. Such a complexity is also reflected in the broad definition of cyber-attack provided in the legal acts at stake,[43] which encompass any act involving access to or interference with information and communication systems. Such acts may include the disruption, deletion, alteration, suppression, or transmission of data, as well as its theft or interception –

[40] C Eckes, 'EU restrictive measures against natural and legal persons: From counterterrorist to third country sanctions' (2014) 51 Common Market L Rev 869-905; S Poli, 'Effective judicial protection and its limits in the case law concerning individual restrictive measures in the European Union', in E Neframi, M Gatti (eds), *Constitutional Issues of EU External Relations Law* (Nomos 2008) 287-306; ME Bartoloni, '"Restrictive Measures" Under Art. 215 TFEU: Towards a Unitary Legal Regime? Brief Reflections on the Bank Refah Judgment' (2020) 5 Eur Papers 1359-1369; Lonardo (n 23).

[41] Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 129I.

[42] ibid.

[43] ibid, art 1. To be noted that the detailed content of these actions broadly corresponds to the offences laid down in the 'Cybercrime Directive' (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, OJ L 218).

covering activities such as data breaches, theft of intellectual property, or financial manipulation.[44]

Beyond definitional issues, however, the operationalisation of the sanctioning mechanism depends on whether specific thresholds are met. Under Article 1 of Decision (CFSP) 2019/797, to activate the sanctioning regime, a cyber-attack must fulfil two criteria: to have a significant effect and to constitute an external threat to the Union or its Member States. However, both requirements raise interpretative and practical challenges. The notion of 'significant effect', for instance, must be assessed with reference to criteria such as disruption to economic or societal activities, material damage, or the type and volume of stolen data.[45] Yet these indicators often fail to capture the full extent – or the potential threshold – of cyber operations. It is particularly difficult to determine when a cyber incident crosses the threshold of severity necessary to trigger restrictive measures, especially in cases where long-term or indirect consequences (e.g., reputational harm, erosion of public trust) are at stake.

Similarly, the fact that a cyber-attack must constitute an 'external' threat presents several challenges.[46] While the reference to the gravity of the effects caused by the attack is familiar in emergency scenarios, the insistence on the external nature of cyber-attacks as a threat to the security of the Union and its Member States is a distinctive feature of the CFSP domain. Indeed, it is a different – and complementary – sanction regime from that related to 'domestic' cyber attacks resulting in internal

[44] Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 129I arts 1(3) and (7).

[45] Council Decision (CFSP) 2019/797 of 17 May 2019 (n 41) art 3.

[46] ibid art 1(2).

threats; indeed, the latter is dealt with under the AFSJ legislative framework, namely the Cybercrime Directive,[47] as happens for the anti-terrorism measures adopted under Council Regulation (EC) 2580/2001.[48] However, while the Decision includes multiple cumulative criteria (such as origin, infrastructure, or actors located outside the EU), the inherently transboundary and anonymised nature of cyber operations makes it difficult to clearly identify the locus of an attack. This ambiguity risks leading either to excessively formalistic interpretations or, conversely, to politically sensitive designations made in the absence of conclusive technical evidence.

In addition to the definitional ambiguity surrounding the nature of the attack, the list of subjects that can trigger the restrictive measures also warrants attention. In fact, for the purposes of the concerned measure, cyber-attacks can be directed not only against entities of the Member States,[49] but also against the EU (institutions, bodies or offices, delegations to third countries or to international organisations, CFDP operations and missions or special representatives). Interestingly, this extension reflects the intention to define a line of protection for the evolving paradigm of the Union's security within the CFSP, parallel to that of the

[47] Cybercrime Directive (n 43). In this regard, it deserves to underline that the European Union is not party to the Council of Europe Convention on Cybercrime (also known as 'Budapest Convention' (adopted 23 November 2001, entered into force 1 July 2004) 2296 UNTS 167) because only States can be parties to that. It, instead, authorised the Member States to ratify the second additional protocol to the Budapest Convention in the interest of the EU (Decision (EU) 2023/436 authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime, OJ L 63). On the contrary, the European Commission has negotiated on behalf of the EU and its Member States the United Nations Convention against Cybercrime that was adopted by the General Assembly of the United Nations on 24 December 2024.

[48] Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism, OJ L 344.

[49] Art 1(4) of Council Decision (CFSP) 2019/797 of 17 May 2019 (n 41) proposes a non exhaustive list of potential entities to be monitored: critical infrastructures; services necessary for the maintenance of essential social and/or economic activities (including energy, transport, banking, health, drinking water supply and distribution, digital infrastructures); critical State functions (defence, governance and the functioning of institutions, the functioning of economic and civil infrastructure, internal security, and external relations); the storage or processing of classified information; and government emergency response teams.

Member States, and to be independently protected against external (cyber) threats.[50] This means that, for example, a significant attack – in the meaning of the referred acts – targeting the electoral process of the European Parliament or seeking to gain access to EU confidential and classified documents, as well as sensitive non-classified information, could determine the activation of this instrument to safeguard the Union's interests. In addition, sanctions may be imposed in response to cyber-attacks with significant effects against third States or international organisations, in the light of the above-mentioned intention to promote internationally a culture of cyber security based on the EU's founding values and to achieve the wider CFSP objectives of Article 21 TEU.[51]

On the basis of Decision (CFSP) 2019/797, in July 2020, the Council listed individuals and entities for three episodes. The first two are related to the cyber-attacks *WannaCry* and *NotPetya* which targeted information networks with ransomware and blocked access to data, thus causing significant economic loss. They were respectively attributed to the North Korean APT38 (Advanced Persistent Threat 38), also known as the 'Lazarus Group', and to the actor publicly known as 'Sandworm' who was connected with the Main Directorate of the General Staff of the Armed Forces of the Russian Federation.[52] The third episode relates to the cyberespionage campaign dubbed *Cloud Hopper* which entailed the theft of industrial and commercial secrets and affected eight of the world's biggest technology service providers. This cyber operation was conducted

[50] Malicious activities can be detected through the mechanisms and services progressively established at the EU level, including the Cybersecurity Service for the Union institutions, bodies, offices and agencies (CERT-EU) and the Interinstitutional Cybersecurity Board (IICB) established under Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, OJ L 2023/2841. Under the supervision of the European Union Agency for Cybersecurity (ENISA), these structures should promote better protection of the ICT environment, by sharing incident-specific information with Member State counterparts and the European cyber crisis liaison organisation network (EU-CyCLONe), as well as by collaborating with other counterparts, including NATO.

[51] Council Decision (CFSP) 2019/797 of 17 May 2019 (n 41) art 1(6).

[52] Council Decision (CFSP) 2020/1127 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States OJ L 246/12; Council Implementing Regulation (EU) 2020/1125 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States OJ L 246/4.

by APT10, which is allegedly linked to the Chinese government. Another two individuals and one body were listed in October 2020 for the cyber-attack against the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Hague which was prevented by Dutch military intelligence, and the German Federal Parliament in April and May 2015; both attributed to Russian cyber agents.[53]

Following the periodic review, the above-mentioned measures have been renewed on an annual basis and none of the above-mentioned individuals or entities have been removed from the EU sanctions list, which has been further extended. Indeed, on 24 June 2024, the Council adopted a new wave of restrictive measures against six natural persons, with also the support of North Macedonia, Montenegro, Albania, Ukraine, the Republic of Moldova and Bosnia and Herzegovina, and the EFTA countries Iceland and Norway.[54] On 27 January 2025, the Council adopted additional restrictive measures against three Russian officers of the General Staff of the Russian military intelligence agency (GRU) Unit 29155, responsible for a series of cyberattacks carried out against the Republic of Estonia in 2020, leading to unauthorized access to non-public information and sensitive data stored within several government ministries.[55]

[53] S Poli, E Sommario, 'The Rationale and the Perils of Failing to Invoke State Responsibility for Cyber-Attacks: The Case of the EU Cyber Sanctions' (2023) 24 German L J 522–536.

[54] Decision (CFSP) 2024/1779 concerning restrictive measures against cyber-attacks threatening the Union or its Member States OJ L, 2024/1779.

[55] Council Decision (CFSP) 2025/171 of 27 January 2025 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States OJ L 2025/171; Council Implementing Regulation (EU) 2025/173 of 27 January 2025 and Implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States OJ L 2025/173. It deserves to be noted that, with regard to the GRU Unit, the mentioned individual measures are currently complemented with those set in Council Decision (CFSP) 2024/2643 in view of Russia's destabilising hybrid activities, which comprise also malicious cyber activities. See, Council Decision (CFSP) 2024/2643 of 8 October 2024 concerning restrictive measures in view of Russia's destabilising activities OJ L 2024/2643; and Council Regulation (EU) 2024/2642 of 8 October 2024 concerning restrictive measures in view of Russia's destabilizing activities OJ L 2024/2642.

4. *The cyber-targeted sanction regime: A double short-circuit for the EU's value-based legal system?*

Representing a relatively recent unilateral instrument for countering and deterring malicious cyber activities, the illustrated targeted sanctions regime is characterised by features that reflect the multifaceted and complex nature of this new threat. Simultaneously, however, it is distinguished by some shortcomings that risk creating a double short-circuit with the attempt to promote and secure the EU constitutional order.

The first element of concern is structural and relates to a classical issue that characterises targeted restrictive measures: the lack of transparency in the listing process and the potential inconsistency with fundamental rights and the principles enshrined in EU primary law. In particular, to be under question are the right to an effective remedy, the right to a fair trial, and the right to the protection of personal data – as reinforced by the Court's case law following the *Kadi* saga and, more recently, in the *Rosneft* case.[56] In essence, when confronted with the issue of cyber-attacks, this paramount concern is compounded by the evident difficulty of accurately geolocating and tracing the origin of the attack.[57] This is a scenario that, although not yet realised, cannot be excluded when dealing with activities in cyberspace. Definitely, this raises questions about the consistency of this external instrument with the EU constitutional con-

[56] Case C-402/05 P *Kadi and Al Barakaat International Foundation v Council and Commission* [2008] ECLI:EU:C:2008:461; Case C-72/15 *Rosneft* [2017] ECLI:EU:C:2017:236. See S Poli, 'The Right to Effective Judicial Protection with Respect to Acts Imposing Restrictive Measures and Its Transformative Force for the Common Foreign and Security Policy' (2022) 4 Common Market L Rev 1045-1080; P Van Elsuwege, 'Securing a Coherent System of Judicial Protection in Relation to Restrictive Measures: Rosneft', in RA Wessel, G Butler (eds), *EU External Relations Law The Cases in Context* (Bloomsbury Publishing 2022) 881-889.

[57] For insights, see E Boebert, 'A Survey of Challenges in Attribution', in *Proceedings of a Workshop on Deterring Cyberattacks* (The National Academies Press 2010) 43; K Mačák, 'Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors' (2016) 21 J Conflict & Security L 405-428.

straints, which are anchored in the very values the Union seeks to protect.[58] Indeed, when cybersecurity has an external connotation, the supranational conduct in this field must not only be oriented to safeguard the security of its principles/values but also to be inspired by them.[59]

The second criticality relates to the process of attribution of the malicious activity to individuals and legal entities, with the consequent adoption of restrictive measures. Indeed, it remains a prerogative of Member States within the Council that, as underlined by the Court of Justice in *Rosneft* case, 'has a broad discretion in determining such persons and entities' but also that, as regards the protection of the essential interests of the Union's security, enjoys a wide discretion when the area of action involves 'the making by that institution of political, economic and social choices, and in which it is called upon to undertake complex assessments.'[60]

Further complicating the picture is the fact that Article 6 of Decision (CFSP) 2019/797 requires the Council to vote by unanimity to establish and amend the list, even though the implementing regulations should be adopted by a qualified majority according to Article 215 TFEU. This choice, which raises serious concerns about the compatibility with the EU Treaties as recently underlined by the European Parliament,[61] is linked to (geo)political and strategic considerations, especially when the adoption of targeted restrictive measures may lead to indirect attribution of responsibility for cyber attacks to a third State.[62] In effect, it is widely

[58] Y Miadzvetskaya, 'Challenges of the Cyber Sanctions Regime under the Common Foreign and Security Policy (CFSP)', in A Vedder, J Schroers, C Ducuing, P Valcke (eds) *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security* (Intersentia 2019) 277-298; I Bogdanova, MV Callo-Muller, 'Unilateral Cyber Sanctions: Between Questioned Legality and Normative Value' (2023) 54 Vanderbilt L Rev 911-954.

[59] A Egan, L Pech, 'Respect for Human Rights as a General Objective of the EU's External Action', in S Douglas-Scott, N Hatzis (eds), *Research handbook on EU law and human rights* (Edward Elgar 2017) 243.

[60] *Rosneft* (n 56) points 88 and 113, by also referring to the case C-348/12 *P Council v Manufacturing Support & Procurement Kala Naft* [2013] ECLI:EU:C:2013:776, point 120; and C-440/14 *P National Iranian Oil Company v Council* [2016] ECLI:EU:C:2016:128, point 77.

[61] Case C-883/24: Action brought on 19 December 2024 – European Parliament v Council of the European Union [2025] OJ C C/2025/899.

[62] For insights on this issue see, *inter alia*, MN Schmitt, Y Shany, 'An International Attribution Mechanism for Hostile Cyber Operations?' (2020) 96 Intl L Studies 196; N

understood that cyber attribution has a technical, political, and legal dimension; and, whereas technical attribution has typically an objective connotation, the criteria to establish political or legal attribution do not always coincide.[63] In this regard, it is interesting (although not surprising) that, according to the Council non-paper on *Attribution of malicious cyber activities*[64] and to Recital 9 of Decision (CFSP) 2019/797,[65] attribution expressly remains a sovereign political decision taken on a case-by-case basis by Member States. This, however, may have some implications on the application of restrictive measures. Indeed, the delimitation between targeted measures and the public attribution of responsibility to a State is rather blurred since a vast majority of cyber attacks with high impact, such as the abovementioned *WannaCry* and *NotPetya*, has been broadly conceived as orchestrated at the request and with the support of governments.[66] And, while not resulting in a legal attribution of State responsibility, national authorities of Member States may be reluctant or otherwise hesitant to recognise the fulfilment of the 'significant effect' criteria and support a collective and shared decision on the application of targeted measures in view of the potential costs in terms of credibility and strategic concerns, especially if they are not directly affected. This scenario, where political and legal reasoning may not always be aligned,

Tsagourias, M Farrell, 'Cyber Attribution: Technical and Legal Approaches and Challenges' (2020) 31 Eur J Intl L 941; A Bendiek, M Schulze, 'Attribution: A Major Challenge for EU Cyber Sanctions' (*SWP*, 16 December 2021) available at <www.swp-berlin.org/10.18449/2021RP11/>; F Delerue, 'Reflections on the Opportunity of an International Attribution and Accountability Mechanism for Cyber Operations' (2024) 106 QIL-Questions Intl L 5.

[63] N Tsagourias, 'Cyber Attribution Agencies: A Sceptical View' (2024) 106 QIL-Questions Intl L 23; I Brunner, 'Attributing cyber operations under International law: Political and legal aspects' (2025) 110 QIL-Questions Intl L 27.

[64] Implementation of the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities - Attribution of malicious cyber activities 6852/1/19 (18 March 2019).

[65] Council Decision (CFSP) 2019/797 of 17 May 2019 (n 41) Recital 9: 'Targeted restrictive measures should be differentiated from the attribution of responsibility for cyber-attacks to a third State. The application of targeted restrictive measures does not amount to such attribution, which is a sovereign *political decision taken on a case-by-case basis*. Every Member State is free to make its own determination with respect to the attribution of cyber-attacks to a third State'.

[66] P Ivan, 'Responding to Cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox' *European Policy Centre* (18 March 2019) available at <www.epc.eu/publication/Responding-to-cyberattacks-EU-Cyber-Diplomacy-Toolbox-218414/>.

is even further replicable when it comes to the delisting process, which is clearly in the hands of Member States and represents the result of compromise rather than objective assessment.[67]

Such uncertainty, due to the high degree of discretion of Member States in the Council, has a significant impact on the effective and real ability to sanction those who commit malicious cyber acts against the EU institutions or bodies for safeguarding the values, security and integrity of the Union as set out in Article 21(2)(a) TEU. Indeed, the Union's security and capacity to protect (but also to promote) its constitutional identity through this CFSP instrument risk being hostage to the compromise between Member States with regard to the adoption of reactive measures against the perpetrators of cyber malicious activities. In effect, as Advocate General Wahl suggested in *H v. Council*, the CFSP has been conceived as *lex imperfecta*[68] and, at this stage, likely inadequate to ensure effective and genuine security of the EU constitutional order, in parallel with that of the Member States.

Pending, among other things, the desire to make greater use within the Council of qualified majority voting in the CFSP in order to avoid blockages in decision-making,[69] it is essential to rely on the general principle of sincere cooperation enshrined in Article 4(3) of the TEU.[70] This principle asks the Union and the Member States, *in full mutual respect*, to assist each other in carrying out tasks that flow from the Treaties. In the field of CFSP, Article 24(3) TEU then specifically requires Member States to support 'the Union's external and security policy actively and unreservedly *in a spirit of loyalty* and mutual solidarity and shall comply with the Union's action in this area' (emphasis added).[71] Furthermore, under Article 32 TEU, 'Member States shall ensure, through the convergence of their actions, that the Union is able to assert its interests and

[67] M Varju, *Between Compliance and Particularism. Member State Interests and European Union Law* (Springer 2019).

[68] Conclusions of Advocate general Wahl of 7 April 2016, Case C-455/14 P *H v Council and Commission* [2016] ECLI:EU:C:2021:978 point 38.

[69] K Pomorska, R A Wessel, 'Qualified Majority Voting in CFSP: A Solution to the Wrong Problem?' (2021) 3 Eur Foreign Affairs Rev 351.

[70] M Klamert, *The Principle of Loyalty in EU Law* (Oxford University Press 2014); F Casolari, *Leale cooperazione tra Stati membri e Unione europea. Studio sulla partecipazione all'Unione al tempo delle crisi* (Editoriale Scientifica 2020).

[71] S Blockmans, 'Differentiation in CFSP' (2013) 66 Studia Diplomatica 53-68.

values on the international scene'.[72] This could imply that, with respect to the need to assert supranational security as an Union's interest, Member States shall behave consistently with their loyalty duties by balancing their interests with those of the EU. This obligation becomes even more important in a context where, as underlined in a passage of the 2022 *Strategic Compass for Security and Defence*, the 'European security is indivisible and any challenge to the European security order affects the security of the EU and its Member States'.[73] The principle of loyal cooperation serves, therefore, to strike a balance between the respect for the prerogatives of Member States in the CFSP and the broader imperative of upholding EU law and pursuing actions that align with the common interest of Union's security in the cyber domain.

5. *Concluding remarks*

In the last Communication on *ProtectEU: a European Internal Security Strategy*, the Commission stressed that 'cybersecurity and technological sovereignty are closely interlinked'.[74] In effect, the Union's recent practice reveals an evolving understanding of technological sovereignty. This development underscores the specificity of EU security needs, particularly in defending its institutional structures and foundational values also against external cyber threats, which may diverge from – and at the same time complement – the national security priorities of the Member States.

In this context, the advancement of EU cyber diplomacy has been crucial not only for protecting the Union and its Member States from hostile cyber operations, but also for promoting a model of cyberspace governance grounded in the rule of law, respect for human rights, and democratic principles. Instruments such as the *EU Cyber Diplomacy Toolbox* and the forthcoming revision of the Blueprint for coordinated

[72] M Gestri, 'Sanctions Imposed by the European Union: Legal and Institutional Aspects', in N Ronzitti (ed), *Coercive Diplomacy, Sanctions and International Law* (Brill/Nijhoff 2016) 70-102.

[73] *A Strategic Compass for Security and Defence* (n 19) 5.

[74] European Commission, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy* (1 April 2025) COM/2025/148 final point 4.

response to large-scale cybersecurity incidents and crises[75] attest to the consolidation of this integrated and strategic approach.

A pivotal component of the Union's legal and political response lies in its capacity to adopt restrictive measures in response to cyber-attacks. Indeed, as the Commission stressed, 'the persistent nature of malicious cyber activity, which often forms part of a wider range of multi-dimensional and hybrid threats, requires continued attention and action at European level'.[76] While Member States retain their sovereign right to respond individually to cyber incidents, coordinated EU-level action enables the adoption of Union-wide sanctions, thereby enhancing the coherence and effectiveness of the collective response. Moreover, as a subject of international law distinct from its Member States, the Union possesses an autonomous capacity to defend its own institutional and security interests through such sanction mechanisms.

This ability to impose targeted restrictive measures illustrates a further step in the attempt to establish a EU technological sovereignty. Traditionally associated with internal regulation in the cyber domain now also encompasses a reactive dimension – namely, the capacity to respond to external interferences threatening the Union's digital security and constitutional identity. In this regard, the ability to identify and sanction the perpetrators of cyber attacks becomes an indispensable element of the Union's sovereignty within its constitutional order. Despite this promising architecture, a number of critical concerns emerge when assessing the actual implementation of the cyber sanctions regime. In effect, while restrictive measures in the cyber domain represent a meaningful step towards a more integrated and value-based legal framework, their effectiveness is inevitably constrained by political discretion, procedural opacity, and a structural dependence on intergovernmental compromise. Given the current fragmented landscape in the CFSP domain, in order to foster a new Union's security culture, a common endeavour is needed on how to institutionally and legally strengthen its capacity to act autonomously and consistently, particularly when the EU institutions and founding values are at stake also in the cyberspace.

[75] *Building Strong Cybersecurity for the EU* (n 4).
[76] *ProtectEU* (n 74).

Abstract: The European Union has gradually developed a complex and evolving legal framework aimed at managing cybersecurity issues, although national security remains an exclusive responsibility of the Member States pursuant to Article 4(2) TEU. Cybersecurity, indeed, represents a specific component of the supranational strategy for a 'Security Union' against exogenous influences that could undermine the EU constitutional order based upon the values set in Article 2 TEU. The article aims to examine recent developments in the Union's cybersecurity instruments under the Common Foreign and Security Policy (CFSP) from a constitutional perspective, considering the EU's value-based legal framework. In particular, the analysis focuses on the adoption of restrictive measures against cyber malicious activities from abroad as instrument of CFSP to counter this type of threat. Based on the challenges that characterise this system of sanctions, the article critically assesses the consistency with the EU's constitutional constraints and its effective contribution to the Union's security, alongside that of the Member States.

Keywords: EU cybersecurity – attribution – restrictive measures – EU values – CFSP