IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Dossier "Europe facing the digital challenge: obstacles and solutions"

EU cybersecurity and cyber diplomacy[1]

Agnes Kasper
Tallinn University of Technology (TalTech)

Anna-Maria Osula
Tallinn University of Technology (TalTech)

Anna Molnár
University of Public Service (Budapest)

Date of submission: May 2021
Accepted in: September 2021
Published in: December 2021

Abstract

Over the last decades cybersecurity has become a cornerstone of European digital development. Alongside with the diffusion of information and communication technologies and the deepening (as well as widening) of the European Union, the initial narrow and sectoral data security policies have expanded into a comprehensive cybersecurity framework addressing issues from resilient infrastructure and technological sovereignty, through tackling cybercrime, to cyber defence capabilities and responsible state behaviour in cyberspace. In this complex web of interrelated policies a relative newcomer at the European Union (EU) level is cyber diplomacy. Sometimes also called public diplomacy 2.0, it factors into the cross-border connectivity of cyberspace and reflects a shift in international relations where the lines between external and internal policies, military and civilian domains are blurred. However, the term cyber diplomacy is fluid and it is not well understood which topics should be under its "umbrella", in particular in relation to cybersecurity, where it seems to be linked the most. This article aims to map

[1] This work was carried out with the support of the Erasmus+ programme of the European Union, CASPA Project (Erasmus+ 2020-1-EE01-KA203-077958). The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects only the views of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

existing and proposed instruments that make up the EU's arsenal in this broad context to answer the following questions: what is cyber diplomacy and how is it related to the EU cybersecurity? Is cyber diplomacy in the EU becoming something in its own right as a distinct set of tools to secure the EU policy objectives?

Keywords

cyber diplomacy; cybersecurity; EU cyber policy; diplomacy 2.0

Ciberseguridad y ciberdiplomacia de la UE

Resumen

Durante las últimas décadas, la ciberseguridad se ha convertido en una piedra angular del desarrollo digital europeo. Junto con la difusión de las tecnologías de la información y la comunicación, y la profundización (así como la ampliación) de la Unión Europea, las políticas de seguridad de datos sectoriales y estrechas iniciales se han expandido a un marco integral de seguridad cibernética que aborda cuestiones de infraestructura resiliente y soberanía tecnológica, mediante la lucha contra la ciberdelincuencia, a las capacidades de defensa cibernética y al comportamiento estatal responsable en el ciberespacio. En esta compleja red de políticas interrelacionadas, un recién llegado en el ámbito de la UE es la ciberdiplomacia. A veces también llamada diplomacia pública 2.0, tiene en cuenta la conectividad transfronteriza del ciberespacio y refleja un cambio en las relaciones internacionales en las que las líneas entre las políticas externas e internas, los dominios militar y civil se difuminan. Sin embargo, el término ciberdiplomacia es fluido y no se comprende bien qué temas tendrían que pertenecer a su "paraguas", en particular en relación con la ciberseguridad, a la cual parece más vinculado. Este artículo tiene como objetivo trazar un mapa de los instrumentos existentes y propuestos que forman el arsenal de la UE en este amplio contexto para responder las preguntas siguientes: ¿qué es la ciberdiplomacia y cómo se relaciona con la ciberseguridad de la UE? ¿Se está convirtiendo la ciberdiplomacia en la UE en algo por derecho propio como un conjunto diferente de herramientas para asegurar los objetivos políticos de la UE?

Palabras clave

ciberdiplomacia; ciberseguridad; ciberpolítica de la UE; diplomacia 2.0

Introduction

Diplomacy has three vectors: agency (who), process (how) and subject matter (what) (Riordan, 2019, p. vii). The contemporary definition of diplomacy also seems to relate to the process of conducting negotiations between representatives of states or international organisations (or non-state actors) (Pigman, 2010, pp. 5-7).

The term 'cyber diplomacy' seems to suggest that it relates to a particular way of dealing with various problems arising in cyberspace. Yet, such problems range from issues of internet governance to addressing cybercrime, from critical infrastructure protection to cyberespionage, cyberconflict, as well as responsible state behaviour in cyberspace, and these do not only refer to state vs state relations. Indeed, if we are about to ask questions on cyber diplomacy in the context of the European Union (EU), we need to take into account that significant variations to the Westphalian concept of state sovereignty are prominent in the EU's existence, and that the virtual lack of physical borders in cyberspace certainly poses both theoretical and practical challenges in understanding sovereignty, and more so for the concept of collective sovereignty.

Since its foundation, the European Union has been described as a *sui generis* international actor, as a unique and complex creature in international relations. While it is not a simple international organisation based on intergovernmental cooperation, it is not a state either. The EU has developed a *sui generis* cyber diplomacy toolbox and framework, a complex web of interrelated policies concerning digital development and cybersecurity which has two prongs. The first element is civilian, as the EU opted for a non-military cybersecurity policy in its Cyber Diplomacy Toolbox in 2017 (Council, 2017); the second element is military, since cyber defence is a *sine qua non* of the new EU Cybersecurity Strategy adopted in December 2020 (Commission, 2020a). Moreover, the Cyber Diplomacy toolbox was the foundation for further proposals on the EU's cyber deterrence posture, which should also give direction countering those cyber-attacks that affect critical infrastructures, democratic institutions and processes, as well supply-chain attacks and cyber-enabled theft of intellectual property – projecting a clear link to the digital single market and its related policies. This points to the widening breath of the concept of cyberdefence, blending military and civilian aspects of cybersecurity, since both the protection of military and civilian assets depend on critical infrastructures, as well as on the integrity of supply chains.

This complexity raises several questions: what are the meaning and scope of cyber diplomacy in the EU context? What are the cyberspace problems the EU aims to address through diplomacy? How is this diplomatic approach related to its cybersecurity policy?

This article maps out existing and proposed instruments that make up the arsenal in this broad context in order to get a first idea of what we can call EU cyber diplomacy. The mapping exercise reveals that the EU cyber diplomacy is a distinct set of tools that reflects the need for the EU to secure its policy objectives. In chapters 1 and 2 we lay foundations regarding global concepts of cyber diplomacy and the EU's cybersecurity policy. In the following chapters (3 and 4) we steer the attention to obvious 'cyber diplomatic' developments in the EU, and we also argue that there is more to EU cyber diplomacy than what meets the eye. We conclude that the EU cyber diplomacy is a function of the political economy driven mainly by the single market.

1. Concept of cyber diplomacy

There are several definitions of the concept of cyber diplomacy in the literature. Summarising the different definitions, cyber diplomacy can be described as diplomacy of cyberspace or the use of diplomatic resources, initiatives and the performance of diplomatic functions to promote national interests that are defined in national cybersecurity strategies. It deals with the international aspects of cyber issues (Barrinha & Renard, 2017, pp. 355-356; Smith & Sutherland, 2002; Manantan, 2021). In the context of the EU, cyber diplomacy aims to promote the adoption of new "norms regulating the behaviour of state and non-state actors in cyberspace" (Cotroneo *et al*., 2021).

The systematic literature review conducted by Attatfa, Renaud and De Paoli (2020, p. 61) concluded that cyber diplomacy relates to resolving issues arising from the international use of cyberspace, and in this process tools of diplomacy and a diplomatic mindset are applied. Although the authors also pointed out the scarcity of relevant literature, whereas only 21 relevant studies written by European and North American authors could be found for intensive analysis, the main dimensions of cyber diplomacy are identified by the following keywords: public, state-led, inter-country ties, coercive power, military, facilitating observation, gathering information, non-governmental (p. 64). It was also noted that so far, no study sought to distinguish cyber diplomacy from the more traditional and well-established diplomacy.

Firstly, data protection-related issues, then more general cyberspace-related matters, national interests and goals are laid down in national and regional cybersecurity strategies. Key issues on the cyber diplomacy agenda typically include the above-mentioned dimension in the context of cybersecurity, cyberdefence, cybercrime, confidence building, internet freedom and internet governance. Key players in cyber diplomacy include traditional diplomats and representatives of the various stakeholders that play a key role in this policy area. As a continuing trend, Ministries of Foreign Affairs are also assigning the role of Cyber Ambassadors to diplomats who are in charge of diplomatic activities and negotiations related to cyber policy (Barrinha & Renard, 2017, p. 3).

As tensions between individual actors and, consequently, between great powers are becoming more frequent in cyberspace today, there is a growing need for international negotiations and agreements to resolve these types of conflict. In recent decades, the EU has played an increasingly active role in this field (Renard, 2018), and for example in September 2021 the High Representative of the Union for Foreign Affairs and Security Policy called upon Chinese authorities to act against malicious cyber activities undertaken from its territory (Council, 2021a).

While the use of ICT (information and communication technology) tools is becoming more widespread at the different levels of foreign affairs administration, cyber diplomacy and e-diplomacy – also known as electronic or digital diplomacy – can be defined as two different concepts. Although the use of the two concepts is often confusing, sometimes these are used as synonyms, there is a significant difference between the two concepts. The main difference is that e-diplomacy or digital diplomacy means the use of digital tools (new technologies and social media) by diplomats and politicians (Molnár, 2020a, p. 344). According to Tom Fletcher, e-diplomacy was officially born in 1994, when Swedish Foreign Secretary Carl Bildt sent his first official diplomatic email to Bill Clinton. The Swedish diplomat thus congratulated the US President on lifting the embargo against Vietnam (Barrinha & Renard, 2017, p. 3). In contrast, Smith and Sutherland use the term of cyber diplomacy to describe increasingly intensive diplomatic activities using digital means. (Smith & Sutherland, 2002, p. 155.) On the other hand, as stated by Ostwald and Dierkes, digital diplomacy means an active presence on Twitter, or on other social media platforms, as digital diplomacy facilitates a "direct person-to-person engagement", which is not possible on a large scale through traditional forms of diplomacy (Ostwald & Dierkes, 2018, pp. 203-206).

Riordan (2019, p. 20) also distinguishes between digital diplomacy and cyber diplomacy by pointing out that the former refers to the promotion of diplomatic agendas by using digital tools, while the latter is the application of diplomacy to the problems arising in cyberspace. He goes further suggesting that the diplomatic approach to cyberspace encompasses a certain way of thinking about and engagement with cyberspace by those who practice cyber diplomacy. It is emphasised that the role and attributes of diplomats in cybersecurity are similar to their role in physical space. However, the argument is put forward that cyber diplomacy is also about developing multi-stakeholder diplomatic capability and it is for the cyber diplomats to build an international cybercommunity to which states and non-state actors will want to belong, and consequently follow the rules of this community (Riordan, 2019, pp. 23-31). Arguably it is the result of such diplomatic community building that in the aftermath of the 2019 October serious cyberattacks against the Georgian social and economic infrastructure, the European Union and its Member States expressed their concern and declared their will to "continue to assist Georgia in increasing its cyber resilience" (Council, 2021b).

Mártonffy (2020) suggests that academic discussions on cyber diplomacy have three focal points according to the traditional international relations paradigms:[2] cyber diplomacy as a function of cybersecurity and more generally

[2] Realism, liberalism, constructivism.

power; cyber diplomacy as a function of economic interdependence, rule of law and international organisations; and finally cyber diplomacy as a function of norms.

Therefore, based on the foregoing, the main distinguishing features of cyber diplomacy may be its subject matter (discussed in the next paragraph), maturity of the field and its likely emerging multi-level and heterogeneous network of actors in this technology-ridden domain. What remains intact is the diplomats' readiness and skill to engage with all manner of actors; and their willingness to accept 'good enough' outcomes since global problems can often only be managed, but not solved (Riordan, 2019, p. 31). The concept and subject matter of cyber diplomacy may also vary depending on one's vantage point and whether the realist, liberal or constructivist thinking is applied.

The only study, to our knowledge, that addresses the broad spectrum of subject matter areas also referred to within the EU's broader cyber policy context is Riordan's work (2019), where cyber diplomacy is divided into four subdomains: (1) internet governance, including purely technical issues, as well as data protection, encryption and content regulation; (2) mitigating cyberconflict or use of cyberspace in conflict between states; (3) business cyber diplomacy; and (4) algorithms and internet companies, on the face of which cyber diplomats arguably need to challenge algorithms. While these subdomains are not a perfect match, they could be discernible for detailed analysis in the EU's context. However, for the purposes of this paper we keep our main focus on the second subdomain, since that relates most explicitly to relations between nation states, while also pointing to some elements in other subdomains.

As to the maturity and actors of the field, and in terms of power, the abilities to shape aspects of the global cybersecurity landscape, it appears that the EU has been on the receiving end when compared with major cyber powers, such as the US and China. The EU's 'soft' powers (also in terms of cyber powers), and lack of 'hard' cyber capabilities at hand may raise questions for some on the credibility of deterrence coming from the EU, but also point to the specific nature of the EU that relies on its persuasive, normative and economic force, its subject-matter expertise and coordinating role (Kasper & Vernygora, 2021).

On the international level, the EU gives great importance to the application of international law to cyberspace, and the implementation of voluntary non-binding cyber norms, rules and principles of responsible state behaviour in cyberspace as agreed in the UN GGE 2013 and 2015 consensus reports (UN 2013; UN 2015). As reflected in the work of UN GGE and OEWG, and in other venues, the EU Member States and the EU itself also promote the development of confidence building measures, capacity building and cooperation with international stakeholders. Importantly, the EU has suggested in its recent Cybersecurity Strategy that its 27 Member States should develop a common EU position on the application of international law in cyberspace (Commission, 2020, p. 20).

2. Brief Overview of the EU's Cyber Policy Framework

According to Carrapico and Barrinha (2018), the EU initiated its activities related to electronic communication and computer security in the second half of the 1990s, but the development of "a fully-fledged approach to cyber security" has only begun in the last two decades. Christou (2018) found that following the distributed denial of service attacks on Estonian private and public institutions and infrastructures in 2007, the EU has been forced to strengthen its approach to cyber security. Since then, a growing number of cyber-attacks against individuals, governmental institutions, companies and critical infrastructures in the EU have increasingly raised awareness of threats and risks related to cyberspace. This process has led to the creation of a comprehensive legal, policy and institutional framework covering all key policy areas of the EU, including cybercrime and cyber defence.

For example, the need to fight against cybercrime has prompted the EU to establish a framework for cooperation at EU level in this area as well. At the beginning of this Millennium, this process was followed by the adoption of legal measures (such as the 2005 Council Framework Decision on attacks against information systems) and the creation of new institutional structures (such as the European Network and Information Security Agency – ENISA in 2004 and the European Cybercrime Center at Europol, EC3 in 2013) (Carrapico & Barrinha, 2018, p. 299). In the domain of defence, there is a growing consensus that the instability and unpredictability characterising the global security environment requires a unified response from the EU and its Member States, including in responding to hybrid threats and cyber-attacks. Here, the latest developments include the review of the Cyber Defence Policy Framework and the upcoming 'Military Vision and Strategy on Cyberspace as a Domain of Operations'.

The EU has developed a complex ecosystem of cybersecurity according to the Union's areas of responsibilities. Article 3 of the Treaty on the EU enshrines the main objectives and policy areas of the Union. These include the promotion of peace and values, the establishment of an area of freedom, security and justice, the completion of the single market, the creation of the eurozone and the promotion of its values in external relations. A multi-level (national, regional and global) system of cybersecurity governance across three distinct policy areas (freedom, justice and security (AFSJ), the internal market, and the Common Security and Defence Policy (CSDP) has emerged (Christou, 2018, pp. 1-2).

According to the report of the European Court of Auditors, the complex ecosystem of the EU's cybersecurity policy is closely linked to internal policy areas, "such as justice and home affairs, the digital single market and research policies. In external policy, cybersecurity features in diplomacy, and is increasingly part of the EU's emerging defence policy" (European Court of Auditors, 2019, p. 12). As cyberspace has become a priority area of international relations, cyber diplomacy has prwoven to be an integral part of the EU's foreign policy toolbox. Activities related to cyber diplomacy mainly concern the Common Foreign and Security Policy (CFSP) and as an integral part of it, the CSDP, but the international representation of cyber security issues related to the internal market and the establishment of an area of freedom, security and justice also belongs to cyber diplomacy. As a result of the comprehensive peculiarity of this issue, practically all institutions, bodies and agencies in the European Union are involved in the preparation and implementation of cybersecurity policy, which is shown below in Table 1.

The European External Action Service (EEAS) is tasked with the management and conducting the diplomatic relations of the EU, having within its competence the CFSP and the CSDP. The EEAS's role is paramount in cyber diplomacy, strategic communication and areas related to cyber defence, and it also hosts the European Union Intelligence Analysis Centre (INTCEN) and the Military Staff Intelligence Directorate, thereby bringing under the same roof intelligence and analysis centres dealing with cyber issues, as well as civilian and military situational awareness. This structure also includes the Hybrid Fusion cell established in 2016 within INTCEN to improve situational awareness and support decision making, and it gathers and analyses classified and open source information concerning hybrid threats (European Court of Auditors, 2019, p. 50; Molnár, 2020b, p. 450).

Having its own complex internal structures, the EU is also actively shaping the legal and policy framework of international cybersecurity, being an actor as well part of the institutional framework at the international level. The next chapter analyses how the core cyber diplomacy pillar of this structure functions.

Cybersecurity in the EU: Areas of responsibility and institutional framework			
Single Market	***Freedom, security and justice***	***CFSP: cyber diplomacy***	***CSDP: cyber defence***
European Commission DGs		EEAS	
CERT-EU	Europol (EC3)	SIAC (EU INTCEN, Hybrid Fusion Cell, EUMS INT)	
ENISA	Eurojust	EU SITROOM	
CSIRT network		ESDC	
	EU-LISA		EDA
			GSA
Source: own elaboration based on Bendiek, 2018, p. 4			

Table 1. Cybersecurity institutional framework in the EU

3. Establishing the Cyber Diplomacy Toolbox

3.1. Emergence of cyber diplomacy in the EU

The international role of the EU related to cyber issues is driven by several foreign policy documents and strategies. The cornerstone of the EU cyber policy is certainly the Cybersecurity Strategy adopted in 2013 (Commission, 2013), and updated in 2020 (Commission, 2020), which aims to ensure the EU's online environment is the safest in the world, protect an open and free internet, and promote cyber-related cooperation with strategic partners, which were at the heart of the negotiations and discussions with United States, Japan, South Korea, India and Brazil (Molnár, 2020, p. 451).

An important milestone in 2015 was the adoption of the Council's conclusions on cyber diplomacy to support the EU's collective efforts (Council, 2015a). For the first time, the EU officially used the term cyber diplomacy, and the Member States agreed that the wide range of issues related to cybersecurity must be addressed in a coherent manner. Such an international cyber policy was foreseen to promote the EU's political, economic and strategic interests and continue international bi- and multilateral discussions with key international partners and organisations as well as the civil society and the private sector. As with all the other cyberspace-related EU's instruments, this development also followed a value-based approach aimed at promoting and protecting a global, open, free, stable and secure cyberspace with a focus on human rights and fundamental freedoms and the rule of law (Council, 2015a, p. 1).

3.2. Growing complexity of the cybersecurity policy and the Cyber Diplomacy Toolbox

One of the challenges related to establishing a cyber policy is the multifaceted nature of cybersecurity which entails a number or specific, yet interlinked topics. For the EU, these topics include the above-mentioned cybersecurity, the promotion and protection of human rights in cyberspace, the application of existing international law, rule of law and norms of behaviour in cyberspace, but also Internet governance, the digital economy, cyber capacity building and development, and strategic cyber relations (Council, 2015a, p. 1). All these domains have their own policies, strategic views and action plans which include the domestic Member State level, the regional EU level and global developments. In order to develop a solid EU cyber policy, the Union needs to achieve greater coherence among Member States and translate the discussions into clear messages to be reflected to external partners. In turn, a common and comprehensive approach to cyber diplomacy can also increase the effectiveness of responses to cyber threats, as well as contribute to conflict prevention and greater stability in international relations. Turning words into action, the 2016 implementation plan on security and defence confirmed this direction and key intelligence bodies within the EEAS turned their attention to cyber issues (Bendiek, 2018, pp. 1-2). Like with other areas of the EU's CFSP, the EU's vision on the governance of cyberspace needs greater visibility, expanding the joined-up approach across policy sectors and demonstrating a veritable union in action among Member States (European Union, 2019, p. 30).

In response to the increased ability and willingness of State and non-state actors to pursue their objectives in cyberspace by carrying out undertaking malicious cyber activities, the EU Cyber Diplomacy Toolbox, that was built on the EU's CFSP Policy Toolbox, was adopted in 2017 (Council, 2017a). This was a significant development for the EU because it established a framework for a joint EU response for malicious cyber activities and outlined the processes for invoking such measures. The aim was to establish a framework for joint EU diplomatic action to facilitate cooperation, promote risk reduction and influence the behaviour of potential attackers, also applying measures used under the CFSP (e.g., restrictive means, aka sanctions). According to the Council conclusions, "a joint EU response to malicious cyber activities would be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity" (Council, 2017b).

Soon after the adoption of the Cyber Diplomacy Toolbox, the Political and Security Committee adopted the corresponding implementing guidelines (Council 2017c), which listed five categories of measures within the Cyber Diplomacy Toolkit. These included restrictive measures and the procedure for imposing such measures, as well as preventive, cooperative, stability measures and possible support to Member States' lawful responses (Council, 2019).

By outlining concrete consequences and thereby aiming to influence the behaviour of possible aggressors, the toolbox serves as classic deterrence. In particular, it is noteworthy that the EU announced that not all measures included in the joint EU diplomatic response to malicious cyber activities require attribution, and that attribution remains a sovereign political decision based on all-source intelligence (Council, 2017a, p. 4).

The measures presented in the guidelines for the implementation of the toolbox are a combination of diplomatic, political and economic actions. These can be used to both prevent or respond to a malicious cyber activity, including in situations where the incident does not rise to the level of internationally wrongful acts but can still be considered as an unfriendly act. The measures can be used independently, or in parallel, either by an individual Member State, collectively with other Member States, by Member States in cooperation with the EU institutions or by the EU institutions themselves. Coordination with like-minded partners and international organisations is encouraged (Council, 2017c, pp. 14-15).

The following section employs the framework of five categories of measures proposed by the 2017 Cyber Diplomacy Toolbox and analyses the EU's activities since the adoption of the document in 2017.

3.3. Implementation

3.3.1. Preventive measures

This group of policy tools includes Confidence Building Measures (CBMs), awareness raising and capacity building. The EU has numerous ongoing initiatives in these areas, both acting as a common voice for the Union and serving individual Member States' objectives, and these are being reflected in several policy documents such as the 2018 Cyber Defence Policy Framework (Council, 2018, p. 8). For example, specifically in the domain of cyber diplomacy, the EU Cyber Diplomacy Support Initiative 2021-2023 aims to promote the EU's position and disseminate its core values via various outreach and capacity building activities with a wide range of stakeholders, both internal and external, governmental and non-governmental. Cyber dialogues, cooperation and sharing best practices take place at bilateral, multilateral and regional fora, covering organisations such as Organisation for Security and Co-operation Europe, ASEAN Regional Forum, Organisation of American States, African Union, G7, and UN bodies as appropriate. Bilaterally, the project underlines the cooperation with the US, China, Japan, the Republic of Korea, India and Brazil (Commission, 2020b).

3.3.2. Cooperative measures

Member States may also make use of the cooperation through EU-led political and thematic dialogues or through démarches by the EU Delegations to signal the seriousness of the situation, facilitate peaceful resolution of an ongoing malicious incident, ask for assistance in mitigating the malicious activity or ask a third country to join in the response to a malicious cyber activity. Such measures could be used for third countries or international organisations (Council, 2017c, p. 7).

An example of a combination of preventive, cooperative and stability functions is the work ongoing within multilateral cyber initiatives and forums. The Cyber Diplomacy Toolbox makes several references to existing EU cyber diplomacy engagement within NATO, the UN and its support to the voluntary norms and guidelines from the UN Groups of Governmental Experts, work of the OSCE (CBMs) and the Council of Europe (Budapest Convention), and others (Council, 2017c, pp. 3-4).

3.3.3. Stability measures

Stability measures include statements by the High Representative and on behalf of the Council of the EU, EU Council conclusions, diplomatic démarches by the EU delegations and signaling through EU-led political and thematic dialogues. All these measures have a signaling effect which underlines awareness, points to the consequences and serves as a form of strategic communication and influence on potential aggressors. For example, Council conclusions can be used to express a political position, to invite another EU institution to take action, or to prepare a proposal for coordinated Member States' action on a specific issue (Council, 2017c, p. 8).

3.3.4. Restrictive measures

Restrictive measures, or sanctions, are designed to influence a change in policy or activity by the target. The target may be a country, government, entity or individual.

Such measures may include travel bans, arms embargoes, freezing funds or economic resources, and the document also mentions the mutual assistance clause of the Lisbon Treaty (Article 42.7). In 2019 the Council of the EU decided to introduce a legal framework for restrictive measures to help improve the response and deterrence capacity of the Union. On 17 May 2019, Council Decision (CFSP) 2019/797 and Council Regulation (EU) 2019/796 were taken on restrictive measures against cyber-attacks threatening the Union or its Member States (Council, 2019a; Council, 2019b). The decision clarifies that the measures in question are within the scope of the CFSP, and the regulation allows the EU to impose sanctions as a response to cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States (Council, 2019a). Thus, the new legal framework allows the EU to impose sanctions such as asset freezing, travel ban, etc. to deter and respond to significant cyber-attacks, however these sanctions need to be effective, proportionate and dissuasive (Commission, 2019, p. 8).

The EU Cyber Diplomacy Toolbox was first used in June 2020. As of May 2021, a total of 8 persons and 4 entities and bodies have been targeted by restrictive measures in relation to cyber-attacks targeting the EU or its Member States.[3] Importantly, the EU is working on further defining its cyber deterrence posture, in particular regarding countering significant cyber-attacks affecting critical infrastructure, democratic institutions and processes. Future work will also include discussions on additional measures for the cyber diplomacy toolbox as well as updating the implementation guidelines. As a reflection of the overarching role of cyber diplomacy, the new EU Cybersecurity Strategy also suggests to "further integrate the cyber diplomacy toolbox in EU crisis mechanisms, seek synergies with efforts to counter hybrid threats, disinformation and foreign interference" (Commission, 2020a).

3.3.5. Possible EU support to Member States' lawful responses

The EU may also support or complement other lawful responses by Member States, carried out individually or collectively. For example, international law offers the victim State, if being the target of an internationally wrongful act, remedies such as the right to launch proportional countermeasures. Member States may also employ their inherent right of individual or collective self-defence as recognised in Article 51 of the Charter of the United Nations or choose to invoke article 42 (7) TEU to call on other Member States to provide aid and assistance, or possibly also engage the solidarity clause.

4. Other areas of cyber diplomacy

The fact that the EU is not a federal state, but a unique and complex creature with limited competences is consequential when addressing questions of cyber diplomacy in and related to the EU. With the EU's 2013 Cybersecurity Strategy it became clear that cybersecurity is regarded as a strategic issue and that it encompasses a broad range of policy areas, as well as levels, and that the complexity of the issues dictates a comprehensive and layered approach. The 2013 Strategy, however, remained preoccupied with cyber threats emanating from the economic sphere. This economic focus fits well with the EU's character and competences. The EU is, after all, a unique economic and political cooperation with the highest density of regular diplomatic interactions (Mauer & Wright, 2020). Unsurprisingly therefore, dialogues and negotiations about cyber issues within the EU and among Member States continued as part of the daily routine. In this respect to treat cybercrime as a concern for 'business cyber diplomacy', as Riordan suggested (2019), makes sense.

Nevertheless, to define cybercrime issues as a problem of the private sector creates the risk to overlook the public interest dimension and thus the importance of international harmonisation on both substantive and procedural rules (such as represented by and progress pursued within the framework of the Budapest Convention). Indeed, in 2021, Europol reported a noteworthy growth in the number of ransomware attacks on public institutions and large companies. On the bases of the reports, we can mention cyber-attacks on public sector organisations in healthcare

[3] 'Malicious Cyber-Attacks: EU Sanctions Two Individuals and One Body over 2015 Bundestag Hack', accessed 6 May 2021, https://www.consilium.europa.eu/en/press/press-releases/2020/10/22/malicious-cyber-attacks-eu-sanctions-two-individuals-and-one-body-over-2015-bundestag-hack/

and education or businesses in finance or energy. The EU institutions have also become the target of these attacks. (Europol, 2021).

Continuing on the idea of the importance of economy and business, Lohmann and other scholars have argued that as a result of declining utility of the use of [kinetic] military force and growing political and economic interdependence, in the 21st century, economic means of state and economic diplomacy were elevated as a preferred policy option to address various threats to national security (Lohmann, 2017). While the EU internal market can be regarded as the ultimate success of economic diplomacy among the Member States, it should also be noted that core issues in cybersecurity have been inseparably linked to the establishment and smooth functioning of the internal market from the outset.[4] The first rules concerning network and information security were in legislation regulating electronic communications, personal data protection, electronic signatures and e-commerce – policy areas clearly within the internal market; however, the cyber aspects were rather secondary and incidental. From 2013 specific measures of cybersecurity policy were adopted, such as the Directive 2013/40/EU on attacks against information systems (that deals with the harmonisation of substantive criminal law, in particular cybercrimes), and they refer back to the need for the "development of the internal market and of a competitive and innovative economy".[5] Even the EU Cyber Defence Policy Framework (2018 update) makes it clear that "several EU policies contribute to the objectives of cyber defence policy…, [such as] the Network and Information Security Directive …which lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market" and the "[Cyber Defence Policy Framework] also takes into account relevant regulation, policy and technology support in the civilian domain" (Council, 2018).

Cyber diplomacy in the EU context has a strong economic element and direct link to the internal market and its policies, and also many policies have a cyber dimension. This complexity has raised questions about the coherence of the EU's cybersecurity policy, as well as about the institutional arrangements on how cyber-related issues are coordinated at different levels. Carrapico and Barrinha (2017) pointed out that the distinction between national, European and global levels is blurred when it comes to cybersecurity, and changes on any of these levels are not without consequences to the others. The EU's 2020 Cybersecurity Strategy resonates with this reality and describes the desired mindset without distinguishing between the levels: "[g]overnments, businesses and individuals need therefore to use digital tools in a responsible, security-conscious manner" (Commission, 2020). Similar ideas of interdependence between the levels are entertained by Troitiño, Kerikmäe and Chochia (2020, p. 209), who argue that further integration is necessary in all those areas, which are implicated in foreign affairs in the EU. Arguably, therefore, cyber diplomacy in the EU encompasses implementation of Member States cybersecurity-related policies on the EU level (which also includes areas where the EU has exclusive competences), as well as coordination and consolidation of such policies with the aim to enhance their effectiveness globally.

Four issues are pointed out here briefly for future reference, which demonstrate both the entanglement of internal and external dimensions, as well as the *sui generis* nature of EU cyber diplomacy: standardisation, internet governance, personal data protection and critical infrastructure protection. All these issues are most closely at the heart of the EU's cybersecurity policy and have strong internal focus, as well as interaction with the international level.

Standardisation efforts are undertaken both in tech and legal contexts. For example, the Cybersecurity Act explicitly addresses cybersecurity standards and certifications, and this is supplemented by other market-focused instruments trying to steer the online presence of businesses towards applying higher security measures (e.g., at least informing consumers about available security updates).[6]

[4] In Case C-217/04 the European Court of Justice considered whether Article 95 EC was the correct choice as a legal basis for the regulation establishing the European Network and Information Security Agency.

[5] Preamble (2).

[6] Directive (EU) 2019/770.

Internet governance issues are very prominent in the 2020 cybersecurity strategy. The EU foresees an ultra-secure quantum communications infrastructure for public authorities, inadvertently expressing low trust in the security of the current networks, and the Commission intends to develop a European DNS resolver service (DNS4EU) to decrease the dependence of the EU on external providers. It also signed up for a particular approach regarding encryption that was set out in a Council resolution, – "security through encryption and security despite encryption" (Council, 2020). Other technical aspects on the use of internet resources and operation of the internet, such as net neutrality, which is arguably a factor limiting the response capabilities of legitimate actors (Hartmann & Giles, 2018, p. 139), as well as several elements (e.g., data retention) in the electronic communications field, remain key, but also controversial issues in cybersecurity. However, the 2020 strategy is careful on interlinking with the mostly market-based personal data protection policy area, as mentions are indirect. However, being aware where the EU's cybersecurity policy started from and also having in regard sections 32-35 of the General Data Protection Regulation (GDPR) on security in particular, the careful rhetoric is no reason to conclude that the GDPR is anything but a cybersecurity tool, which has effects both within the EU as well as externally.

Conclusions

The EU cyber diplomacy is ultimately a function of economic interdependence both at global, as well as intra-EU levels, whose focus is a natural consequence of the Union's *sui generis* character. Consequently, it relates to a broad spectrum of cybersecurity policy areas: its non-military cyber policy, its heavy reliance on its economic might and market-oriented solutions, as well the EU's normative power and appeal in cybersecurity-related areas. The EU cyber diplomacy areas derive their relevance from the central importance of the single market and the protection of fundamental rights. Therefore, the EU cyber diplomacy deals with reducing cyber threats to the (digital) single market and the protection of fundamental rights; as well as reducing the EU's own vulnerabilities and weaknesses that expose these areas to harms originating from cyberspace. Engagement in the normative discussion on international cybersecurity by the Union is in line with its character and given its lack of offensive cyber capabilities and technological reliance on external actors, its tools to reduce cyber threats are naturally limited. Hence, the internal focus and reduction of vulnerabilities internally and building resilience at the level of Member States needs to be an integral part of the EU's cyber diplomacy.

Similarly to cybersecurity, cyber diplomacy is a multi-layered concept and needs to be developed keeping in mind the interrelations between different subtopics related to cyber policy. To promote more coherent policy messages and goals, cyber diplomacy should keep away from compartmentalisation and aim for a comprehensive approach. As has been demonstrated by this article, cyber diplomacy has become an integral part of CFSP and issues related to cyber policy should therefore be part of all negotiations.

Developments in the EU also point at the increasing relevance of assisting Member States with effective responses for malicious cyber incidents. The EU's objective is to develop its cyber deterrence posture, in particular regarding countering significant cyber-attacks affecting critical infrastructures, democratic institutions and processes. It also promotes discussions on additional measures for the cyber diplomacy toolbox and clear steps towards a stronger cyber diplomacy stance and a more resilient Union.

References

ATTATFA, A.; RENAUD, K.; DE PAOLI, S. (2020). "Cyber Diplomacy: A Systematic Literature Review". In: *Procedia Computer Science*, vol. 176, pp. 60-69 [online]. ISSN 1877-0509. DOI: https://doi.org/10.1016/j.procs.2020.08.007

BARRINHA, A.; RENARD, T. (2017). "Cyber-diplomacy: the making of an international society in the digital age". In: *Global Affairs*, vol. 3, no. 4-5, pp. 353-364 [online]. DOI: https://doi.org/10.1080/23340460.2017.1414924

BENDIEK, A. (2018, April). "The EU as a Force for Peace in International Cyber Diplomacy". In: *SWP Comment*, no. 19, pp. 1-2 [online]. Available at: https://www.swp-berlin.org/fileadmin/contents/products/comments/2018C19_bdk.pdf [Accessed: 14 May 2021]

CARRAPICO, H.; BARRINHA, A. (2017). "The EU as a Coherent (Cyber)Security Actor?". In: *JCMS*, vol. 55, no. 6, pp. 1254-1272 [online]. DOI: https://doi.org/10.1111/jcms.12575

CARRAPICO, H.; BARRIHNA, A. (2018). "European Union cyber security as an emerging research and policy field". In: *European Politics and Society*, vol. 19, no. 3, pp. 299- 303 [online]. DOI: https://doi.org/10.1080/23745118.2018.1430712

CHRISTOU, G. (2018). "The collective securitisation of cyberspace in the European Union". In: *West European Politics*, vol. 42, no. 2, pp. 1-24 [online]. DOI: https://doi.org/10.1080/01402382.2018.1510195

COTRONEO, C. *et al*. (2021). "EU Cyber Diplomacy 101". In: *EIPA* [online]. Available at: https://www.eipa.eu/eu-cyber-diplomacy-101/ [Accessed: 8 September 2021]

COUNCIL OF THE EUROPEAN UNION (2015b). "Malicious Cyber-Attacks: EU Sanctions Two Individuals and One Body over 2015 Bundestag Hack" [online press release]. Available at: https://www.consilium.europa.eu/en/press/press-releases/2020/10/22/malicious-cyber-attacks-eu-sanctions-two-individuals-and-one-body-over-2015-bundestag-hack/ [Accessed: 14 May 2021]

COUNCIL OF THE EUROPEAN UNION (2017b). "Cyber attacks: EU ready to respond with a range of measures, including sanctions" [online press release]. Available at: https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/pdf/ [Accessed: 14 May 2021]

COUNCIL OF THE EUROPEAN UNION (2021a). "China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory" [online press release]. Available at: https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/ [Accessed: 9 September 2021]

COUNCIL OF THE EUROPEAN UNION (2021b). "Declaration by the High Representative on behalf of the European Union - call to promote and conduct responsible behaviour in cyberspace" [online press release]. Available at: https://www.consilium.europa.eu/en/press/press-releases/2020/02/21/declaration-by-the-high-representative-on-behalf-of-the-european-union-call-to-promote-and-conduct-responsible-behaviour-in-cyberspace/ [Accessed: 9 September 2021]

EUROPEAN COURT OF AUDITORS (2019, March). "Challenges to effective EU cybersecurity policy, Briefing Paper" [online]. Available at: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf [Accessed: 14 May 2021]

EUROPOL (2021, 12 April). "European Union serious and organised crime threat assessment" [online]. Available at: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment [Access: 9 September 2021]

HARTMANN, K.; GILES, K. (2018). "Net Neutrality in the Context of Cyber Warfare". In: MINÁRIK, T.; JAKSCHIS, R.; LINDSTRÖM, L. (eds.). *10th International Conference on Cyber Conflict CyCon X: Maximising Effects*, pp. 139-158 [online]. Tallinn: NATO CCD COE Publications. DOI: https://doi.org/10.23919/CYCON.2018.8405015

KASPER, A.; VERNYGORA, V. (2021). "The EU's cybersecurity: a strategic narrative of a cyber power or a confusing policy for a local common market?". In: *Cuadernos Europeos de Deusto - DEUSTO Journal of European Studies*, no. 65, pp. 29-71 [online]. DOI: https://doi.org/10.18543/ced-65-2021pp29-71

LOHMANN, S. (2017). "Understanding diplomacy in the 21st century". In: *Working Paper*, no. 11 [online]. Available at: https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/WP_Diplomacy21_No11_Sascha_Lohmann_01.pdf [Accessed: 14 May 2021]

MANANTAN, M. B. F. (2021). "Defining Cyber Diplomacy". In: *Australian Institute of International Affairs* [online]. Available at: https://www.internationalaffairs.org.au/australianoutlook/defining-cyber-diplomacy/ [Accessed: 8 September 2021]

MÁRTONFFY, B. (2020). "Cyberdiplomacy: A Review from the Literature". In: TÖRÖK, B. (ed.). *Információ és kiberbiztonság*, pp. 409-436 [online]. Budapest: Ludovika Egyetemi Kiadó. Available in: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf;jsessionid=FEFF1CE7C622E2DE953BFE3AA5AC1D59?sequence=1

MAURER, H.; WRIGHT, N. (2020). "A New Paradigm for EU Diplomacy? EU Council Negotiations in a Time of Physical Restrictions". In: *The Hague Journal of Diplomacy*, vol. 15, no. 4, pp. 556-568 [online]. DOI: https://doi.org/10.1163/1871191X-BJA10039

MOLNÁR, A. (2020a). "A kiberdiplomácia fejlődése az Európai Unióban". In: TÖRÖK, B. (ed.). *Információ és kiberbiztonság*, pp. 343-356. Budapest: Ludovika Egyetemi Kiadó. Available at: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf;jsessionid=FEFF1CE7C622E2DE953BFE3AA5AC1D59?sequence=1

MOLNÁR, A. (2020b). "European Union – Cybersecurity". In: TÖRÖK, B. (ed.). *Információ és kiberbiztonság*, pp. 437-456 [online]. Budapest: Ludovika Egyetemi Kiadó. Available at: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf;jsessionid=FEFF1CE7C622E2DE953BFE3AA5AC1D59?sequence=1

OSTWALD, K.; DIERKES, J. (2018). "Canada's foreign policy and bureaucratic (un)responsiveness: public diplomacy in the digital domain". In: *Canadian Foreign Policy Journal*, vol. 24, no. 2, pp. 202-222 [online]. DOI: https://doi.org/10.1080/11926422.2018.1461664

PIGMAN, G. A. (2010). *Contemporary Diplomacy*. Cambridge: Polity Press.

RAMIRO TROITIÑO, D.; KERIKMÄE, T.; CHOCHIA, A. (2020). "Foreign Affairs of the European Union: How to Become an Independent and Dominant Power in the International Arena". In: RAMIRO TROITIÑO, D.; KERIKMÄE, T.; DE LA GUARDIA, R.; PÉREZ SÁNCHEZ, G. (eds). *The EU in the 21st Century* [online]. Cham: Springer. DOI: https://doi.org/10.1007/978-3-030-38399-2_12

RENARD, T. (2018). "EU cyber partnerships: Assessing the EU strategic partnerships with third countries in the cyber domain". In: *European Politics and Society*, vol. 19, no. 3, pp. 1-18 [online]. DOI: https://doi.org/10.1080/23745118.2018.1430720

RIORDAN, S. (2019). *Cyberdiplomacy: Managing Security and Governance Online*. Cambridge: Polity Press.

SMITH, G.; SUTHERLAND, A. (2002). "The New Diplomacy: Real-Time Implications and Applications". In: POTTER, E. H. (ed.). *Cyber-diplomacy: managing foreign policy in the twenty first century*, p. 151-177 [online]. Quebec: McGill-Queen's University Press. DOI: https://doi.org/10.1080/11926422.2002.9673306

Case law, legal and policy documents

Commission 2019, European Commission, Joint Communication to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, Report on the implementation of the Action Plan Against Disinformation, JOIN (2019) 12 final.

Commission 2020a, European Commission, Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, JOIN (2020)18 Final.

Commission 2020b, European Commission, Action Document for EU Cyber Diplomacy Support Initiative, Annex 9 of the Commission Implementing Decision on the 2020 Annual Action programme for the Partnership Instrument.

Council 2015a, Council of the European Union, 'Draft Council Conclusions on Cyber Diplomacy', 2015.

Council 2017a, Council of the European Union, 'Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")', 2017.

Council 2017c, Council of the European Union, 'Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities', 2017.

Council 2018, Council of the European Union, EU Cyber Defence Policy Framework, 2018.

Council 2019a, Council Decision (CFSP) 2019/797 of 17 May 2019, concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

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

Council 2020, Council Resolution on Encryption - Security through encryption and security despite encryption, 13084/1/20 REV 1.

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, 14.8.2013, p. 8–14.

Directive 2019/770/EU of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services. PE/26/2019/REV/1. OJ L 136, 22.5.2019, p. 1–27.

European Union, The European Union's Global Strategy: Three Years on, Looking Forward', 2019.

Judgment of the Court (Grand Chamber) of 2 May 2006. United Kingdom of Great Britain and Northern Ireland vs European Parliament and Council of the European Union. Regulation (EC) No 460/2004 - European Network and Information Security Agency - Choice of legal basis. Case C-217/04.

United Nations, Group of Governmental Experts, Developments in the field of information and telecommunications in the context of international security, 2013, A/68/98*.

United Nations, Group of Governmental Experts, Developments in the field of information and telecommunications in the context of international security, 2015, A/70/174.

Recommended citation

KASPER, Agnes; OSULA, Anna-Maria; MOLNÁR, Anna (2022). "Cyber security and EU cyber diplomacy". *IDP. Internet, Law and Politics E-Journal*. No. 34. UOC [Accessed: dd/mm/aa] http://dx.doi.org/10.7238/idp.v0i34.387469

About the authors

Agnes Kasper
Tallinn University of Technology (TalTech).
agnes.kasper@taltech.ee

Senior Lecturer of Law and Technology in the Department of Law of Tallinn University of Technology (TalTech). She holds a BA in International Business, MA in Law and Ph.D. in Management, and received formal trainings on technical aspects of cybersecurity and digital evidence. Dr Kasper teaches subjects such as cybersecurity and law, IT contracts, digital evidence. Her current research focuses on regulatory aspects of cybersecurity and she is the lead coordinator for Erasmus+ project "Cyber Aware Students for Public Administrations" (CASPA).

CASPA Project (Erasmus+ 2020-1-EE01-KA203-077958)

Anna-Maria Osula
Tallinn University of Technology (TalTech)
anna-maria.osula@ttu.ee

Senior policy officer at Guardtime, with a focus on cyber security policy and regulation, and supporting international R&D projects. She also serves as a senior researcher at Tallinn University of Technology (TalTech), and as a research fellow at Masaryk University under the project "Cyber Security, Cyber Crime and Critical Information Infrastructures Center of Excellence". Previously, she worked as a legal researcher at the NATO CCDCOE, focusing on national cyber security strategies, international organisations, international criminal cooperation and norms. In addition to a Ph.D. in law from the University of Tartu, she holds an LLM degree in IT law from Stockholm University.

CASPA Project (Erasmus+ 2020-1-EE01-KA203-077958)

Anna Molnár
University of Public Service (Budapest)
molnar.anna@uni-nke.hu

Professor at the University of Public Service (Budapest) and Head of the Department of International Security Studies. She is the Head of the International Public Management bachelor›s program and the International Public Service Relations Master. She was the Head of Programme of MA in international studies at the University of Pannonia between 2010 and 2013. She received her Ph.D. in international relations from the Corvinus University of Budapest (2003). Her published papers cover a wide range of topics focusing on security studies, EU CFSP/CSDP, cyber security, Europeanization of Hungary, and Italian politics.

CASPA Project (Erasmus+ 2020-1-EE01-KA203-077958)

Universitat Oberta de Catalunya