The European Union as a Global Actor in Cyberspace: Can the Cyber Sanctions Regime Effectively Deter Cyber-Threats?

Martina CALLERI
Cyber Security Consultant
martinacalleri94@gmail.com

Abstract: This paper presents and analyses the cyber sanctions regime of the European Union (EU) approved by the Council of the EU on May 17, 2019. The broader aim is to explore the effectiveness of the EU's approach towards cyber diplomacy. To do so, the strategy and means leveraged by the EU to influence the behaviour of potential aggressors in cyberspace are analysed.

The first argument is that the EU's ambitions as a global actor in cyberspace are not met by its cyber-defence capabilities. As for similar challenges that the EU is facing in the realm of the Common Foreign and Security Policy (CFSP), there is a capability-expectations gap *[Hill, 1993]* in cyber-defence.

Important actions have been taken to recognise the importance of a free, open and secure internet. Nevertheless, more capabilities are needed to dissuade state actors from carrying out cyber-attacks against EU assets. The final part of the paper aims to explore how the cyber sanctions regime tackles the need to fill the EU's capability-expectation gap in cyber-defence.

Keywords: cyber security, cyber sanctions regime, cyber defence

INTRODUCTION

Digitalisation has the vast potential to foster economic and employment growth, as well as to act as an important lever of social integration. This process, however, is not exempted from risks and uncertainties. The World Economic Forum's 2019 global risks report places cyber among the top five likely risks and top 10 most impactful risks *[World Economic Forum, 2019]*.

As cyber-attacks from both state and non-state actors are on the rise, analysts already observe and, furthermore, predict the change of traditional warfare. The race to digital supremacy is ongoing, but technology is already emerging as one of the enablers of sovereignty and a cornerstone of defence in all five domains of warfare: land, air, sea, cyber and space. Even if cyber warfare may not entirely replace kinetic warfare, it will constitute an increasingly sophisticated tactic to support military strategies *[Cirlig, 2014]*.

For the purpose of this paper, cyber warfare consists of:

• 'cyber means' or cyber weapons that can cause physical death and material destruction and;

• 'cyber methods' or the tactics, techniques and procedures used to achieve sovereignty in the cyberspace.

In the absence of an international regime on cyber-norms, the definition of the *Tallin Manual [Schmitt, 2013]* appears as the most consistent with traditional warfare doctrine. Moreover, the non-legal term 'cyber operation' will be used to describe all kinds of malicious cyber activity that fall under the threshold of 'armed attack', which sets the condition for the right of self-defence under International Humanitarian Law (IHL). This 'cyber operation' definition encompasses the offensive operations conducted by China, Russia, Iran, North Korea and other state-actors. While the cyber-arena has increasingly become militarised and, hence, a new frontier to be defended, these countries are considered an external threat by the EU and the United States. They use cyber methods to undermine the stability of democracies, "insidiously leveraging the inherent difficulty in attributing cyber-attacks" *[Rugge, 2018].*

The lack of clear rules of the cyber-game, the relative low cost and ease to set and launch the respective cyber operations poses a challenge to the EU. How can the EU effectively deter cyber-attacks in the absence of an effective strategy of deterrence and of a global regime regulating the response to offensive operations? Traditional deterrence theory can offer an explanation for this conundrum. According to Joseph Nye, deterrence is about "dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit" *[Nye, 2015].* An effective strategy of deterrence is based on two elements: credible threat and denial. Firstly, the threat must depict a credible punishment for an action *[Schelling, 1960].* This is, for example, the case with nuclear weapons. During the Cold War, global powers effectively made the argument that the deployment of nuclear weapons by one would have led to imminent mutual destruction. As for cyber-weapons, can the EU effectively communicate and sustain a certain 'fear of retaliation' to adequately and credibly counter cyber-operations? The second element of deterrence, 'denial', consists of preventing action on the part of adversaries by fear of consequences inflicted during the act of aggression and in the same place *[Snyder, 1961].* In other words, deterrence is about denying a net benefit ratio to the attackers. In such case, is the EU duly equipped to adequately and proportionately defend amidst cyber-operations?

In this paper, I address the challenge to develop an effective strategy of deterrence to counter cyber-operations targeting the EU Member States and the European Institutions. Firstly, I argue that there is a capability-expectation gap *[Hill, 1998]* in the EU's cyber-defence capabilities. This undermines the EU's actorness in the cyberspace. Secondly, I demonstrate that cyber-operations carried out against European infrastructures, assets and stakeholders have a high payoff with relatively small risks, being highly suitable for asymmetric warfare. In the absence of a well-defined strategy and of an international regime on cyber-warfare, the EU lacks the means to present a clear response to offensive operations. To conclude, I assess whether the newly approved cyber-sanctions regime contributed to raising the costs of conducting cyber-operations.

THE EU CAPABILITY-EXPECTATION GAP IN CYBERSPACE

State-sponsored operations against EU members and institutions are increasing in both frequency and magnitude. Mainly originating from Russia, China, Iran, Turkey and North Korea, cyber-operations undermine the stability of the Digital Single Market by means of cyber-espionage, critical infrastructure vulnerability scanning and disruptive attacks *[Moret, 2017].* Such activities may constitute wrongful acts under international law and could trigger a joint EU response.

In this section, I present the EU strategy for a safe, open and secure cyberspace. Initially, the EU cyber security strategy has focused on "keeping cyberspace open, free, stable

and secure" *[Council Conclusions, 2017]*. In 2012, the former High Representative of the Union for Foreign Affairs and Security Policy/ Vice-President of the European Commission, Catherine Ashton, stated that "this vulnerability of our societies is bound to attract destructive forces". The 2013 EU's Cyber Security Strategy (EUCSS) aimed at harmonising "the readiness of EU countries to deal with the security challenges in cyberspace". The EUCSS was updated in 2017 with the aim to improve the protection of Europe's critical infrastructure.

As a second step for a more resilient EU, the European Commission has created the basis for a strategy to counter cyber-crime that represents a systemic risk to the stability of the Digital Single Market. 2017 was particularly relevant for cyber policy-making as several initiatives gained momentum. That year, the European Commission launched the Cybersecurity Package, that includes provisions on a permanent mandate to the EU Agency for Network and Information Security (ENISA); an EU cybersecurity certification framework; full implementation of the Directive on Network and Information Security; a blueprint for rapid emergency response; establishing EU-wide cyber-research centres; improving law-enforcement response; and improving the overall resilience of the Union. The pace in which these initiatives were approved shows that the EU is mature enough to recognise the dangers of cyberspace and act upon them.

If, on one side, the European Commission is taking action to protect the Digital Single Market, on the other, Member States in the Council are hanging on to national prerogatives. In terms of military capabilities, EU countries would need a greater pool of resources to build a cyber-arsenal. There are currently some 2,500 to 3,500 soldiers in the European cyber-forces (Munich Security Conference, 2019), with significant differences between countries in terms of national cyber capacity. The number is low when compared to the size of the US Cyber Command that is about twice as large and was expected to grow substantially in 2019 *[Breene, 2016]*. To maximize European efforts in cyber capacity-building, an estimated $2 to $3 billion annually invested in cyber-means will be required *[MSC, 2019]*.

From these estimates, it appears evident that a certain capability-expectation gap *[Hill, 1998]* exists in the EU cyber-defence. Since the beginning of the EU policy-making on cybersecurity, the cyber-institutional framework of the EU has evolved into a decentralised system governed by Member States. At the EU level, the institutions and agencies support capacity building, ensure consistency across Member States, and facilitate co-ordination and outreach *[Carrapico, 2017]*. Nevertheless, the EU cannot support its ambition to dissuade malicious actors from their cyber-activity. The lack of means to support the EU strategy in cyberspace lowers the costs for an attack, providing an incentive for the proliferation of cyber-attacks. Looking at the cyber-capabilities of the EU, cyber-actors will not be discouraged from attempting an attack. For this reason, the EU cannot achieve 'deterrence by denial' through its defence capabilities. It still lacks the capabilities to deny the benefits of cyber-attacks. In the next paragraph, I will present the diplomatic instruments that the EU adopts to build up its deterrence in the absence of a full-fledged cyber-defence.

THE EU STRATEGY OF CYBER-DETERRENCE BY DENIAL

The EU makes use of diplomatic resources and functions to project and coordinate Member States' national interest in cyberspace *[Barrinha, 2017]*. Cyber diplomacy is part of the EU strategy of deterrence by denial, whose aim is to influence the behaviour of cyber-criminals by signalling them that their illegal actions will have consequences *[Nye, 2017]*. The EU also aims to reach international consensus to promote a responsible behaviour in cyberspace. In the Council Conclusions on Cyber Diplomacy (2015), Member States framed the objective to develop a "coherent international cyberspace policy that promotes EU political, economic and

strategic interests and continue to engage with key international partners and organisations as well as with civil society and the private sector" *[General Secretariat of the Council, 2015]*.

To diminish the likelihood of cyber-attacks, the EU pursues a twofold strategy by advocating for its normative posture on the global stage and developing a diplomatic framework to respond to cyber-attacks. Firstly, EU Member States have taken steps to communicate to external actors that malicious cyber activities may "constitute wrongful acts under international law and could give rise to a joint EU response". Member States take part to the United Nations' discussions on how to apply international norms in cyber-space. Although, discussions in the United Nations Security Council are stuck on the problem of attribution.

Attribution in the cyber-arena is made difficult by the technical architecture and geography of the Internet on one side, and the general disagreement among countries on which norms of international law do apply to cyberspace. European countries have sided with the United States in communicating their view on the matter. The United States has promoted the view that International Humanitarian Law (IHL) applies in cyberspace. The 2017 G7 Declaration on Responsible States Behaviour in Cyberspace stated that "in the interest of conflict prevention and peaceful settlement of disputes, international law also provides a framework for States' responses to wrongful acts that do not amount to an armed attack" *[G7/8 Foreign Ministers Meetings, 2017]*. Under IHL provisions, deliberate attacks on civilians are prohibited and, hence, cyber-operations that do not cause the loss of lives or material destruction would still be unlawful. Several academic experts have supported this view. Among them, Taddeo (2014) attempted to fill the conceptual vacuum surrounding cyber warfare by arguing that international law already contains the necessary provisions to regulate the cyberspace. Reputational costs can dissuade state-actors from conducting cyber-operations. By taking part in cyber dialogues, the EU sends a signal to external actors that a given attack can damage a country's reputation on the international stage beyond the immediate impact of the cyber-incident it causes *[Nye, 2017]*.

In deterrence theory, a threat must be credible to fulfil a deterring effect. Accordingly, as a second step in building cyber deterrence, the EU has supported normative action by setting up a diplomatic framework to respond to cyber-attacks. In 2017, the Council agreed to develop the EU Cyber Diplomatic Toolbox, establishing a framework for a "joint diplomatic response to malicious cyber activities" *[Council of the European Union, 2017]*. In the next section, I will analyse the core of the Diplomatic Toolbox of the EU: the restrictive measures against cyber-attacks threatening the Union or its Member States *[Council of the European Union, 2019]*.

THE CYBER SANCTIONS REGIME

To form an effective diplomatic response to cyber operations, the EU needs to make full use of measures within the Common Foreign and Security Policy (CFSP). Accordingly, on May 17, 2019, the Council of the EU established the cyber sanctions regime *[Council of the European Union, 2017]*. The legal provisions for restrictive measures are contained in the Article 21 of the Treaty on the EU (TEU), which details them as a valuable instrument to pursue CFSP.

The framework allows the EU to impose targeted restrictive measures to deter and respond to cyber-attacks, which constitute an external threat to the EU, its Member States, third States or international organisations. As a first reaction to the Council's decision, North Macedonia, Montenegro, Serbia, Albania, Bosnia and Herzegovina, Iceland, Norway and Georgia aligned with this decision *[Council of the European Union, 2019]*. The regime could be endorsed by more States as the EU builds consensus on responsible states' behaviour in cyberspace.

The process for listing individuals under the cyber sanctions regime mirrors the one that

applies to restrictive measures in general. Countries will need to agree that evidence provided on a cyber-attack "surpasses the threshold of a sufficiently solid factual basis that an individual or entity meets the listing criteria in any given circumstances" *[Politico, 2018]*. The regime does not set provisions for intelligence gathering, which still remains a national prerogative.

The EU sanctions regime will rely on forensic evidence and lessons learnt to build a case for applying restrictive measures. For the purpose of assessing the impact and building the case for applying restrictive measures, States will need to cooperate with the private sector. The support of private actors for the regime could go beyond the purpose of information gathering. The EU sanctions regime requires Member States to assess if an incident has a "significant effect". In 2018, following the implementation of the Directive on Network and Information Security (NIS Directive), the operators of essential services dealt with defining which attacks have a "significant impact". Lessons learnt can be drawn from them to implement the EU sanctions regime.

As a matter of fact, the incidents' severity assessment is performed both on the basis of qualitative and quantitative parameters leading to ambiguity in what constitutes a 'significant' impact. In an NIS Directive Compliance Survey conducted by Deloitte (2020), respondents indicate that the three main parameters, considered by more than 80% of organisations to determine whether a cyber-attack has a significant effect, are: the number of users affected by the incident, the duration of the incident and the extent of the disruption of the service. Close behind, more than 60% of organisations consider the geographical spread of the attack and the impact on other economic and societal activities, which could hint at an oversight to the dependencies and interdependencies of cyber incidents. Almost 40% of respondents stated that they consider other indicators when assessing cyber incidents.

While the effectiveness of the regime will be measured against its implementation, some considerations on its limits can already be made. The cyber sanctions regime deals with forensic attribution – as opposed to political attribution. Forensic attribution is about tracing back the attack to the agent. Political attribution is about assigning responsibility for a malicious cyber activity to a specific actor. While forensic attribution is based on evidence, political attribution involves economic and social aspects, too. After responsibility has been assigned, attribution may lead to an either public or confidential diplomatic response. However, not all cases may trigger attribution, as it remains a sovereign decision, dependent on states' national interests.

As noted by the European Policy Centre (2019), the Council Decision concerning restrictive measures allows the EU to adopt individual sanctions against perpetrators of a cyber-attack without attributing the "responsibility for cyber-attacks to a third State" *[Council of the European Union, 2019]*. The logic underneath was that "not all diplomatic measures require attribution" *[Council of the EU, 2019]*. With the cyber sanctions regime, the EU is equipped to express concerns for a cyber-operation and signal it without attributing the attack to the state mandating it, if any.

Nevertheless, a coordinated attribution at EU level will require consensus amongst all Member States. Indeed, the process of listing sanctioned individuals requires unanimity in the Council. Unanimity could imply that, when being presented with forensic evidence, Member States could still raise political concerns. This could endanger the effectiveness of the regime and, ultimately, the EU actorness in cyberspace.

As noted by the Assistant Secretary General for Emerging Security Challenges, Antonio Missiroli, in regards with the EU capacity to behave as a global actor, it "has often achieved unanimity at the expense of effectiveness" *[Missiroli, 2001, p. 5]*. Indeed, as described in this paper, numerous coherence problems observed in traditional CFSP have spilled over into cybersecurity.

Nevertheless, in the absence of an international regime on cyber norms, the cyber sanctions regime has the potential to convey the EU's cyber posture on the world stage. By signalling to cyber-criminals that their actions will not be left unpunished, the EU can communicate its views to state-actors. In so doing, the EU would promote the application of existing international law, in particular the United Nations' Charter in its entirety, in cyberspace, the development and implementation of universal non-binding norms of responsible state behaviour, and regional confidence building measures (CBMs) between States. Diplomatic action could increase transparency and reduce the risk of misperceptions in States' behaviour, ultimately helping the EU in building a credible deterrence amidst cyber-threats.

CONCLUSION

In a non-paper, Denmark, Estonia, Finland, Latvia, Lithuania, the Netherlands, Romania, and the United Kingdom jointly state that "[i] It is only a matter of time before we are hit by a critical operation with severe consequences on the EU and Member States" *[Politico, 2018]*. The EU must be able to both create a credible deterrent and respond to malicious cyber-activity and be rightfully equipped with the tools to dissuade actors from attempting such attacks.

To do so, the EU aims to build resilience, on one side, and to signal that there are consequences to breaking the norms of responsible behaviour in cyberspace, on the other. This paper presented the argument that the EU has a capability-expectation gap in cyber-defence. The EU ambition to become a global actor in cyberspace is not met by its current capabilities. In this context, cyber diplomacy constitutes an effective tool of cyber-deterrence.

The EU Cyber Diplomatic Toolbox and its provisions on restrictive measures increase the costs of coercive cyber operations and establish a deterrent effect (Council of the EU, 2016). While this instrument does not fully deter cyber-methods, it has the potential to influence normative discussions on cyberwarfare.

REFERENCE LIST

Barbieri, C., Darnis, J., & Polito, C. (2018). Non-proliferation Regime for Cyber Weapons. A Tentative Study, Istituto Affari Internazionali. Retrieved from http://www.iai.it/sites/default/files/iai1803.pdf

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: The making of an International Society in the Digital Age. Global Affairs. Volume 3 (Issue 4-5). https://doi.org/10.1080/23340460.2017.1414924

Breene, K. (2016). Who are the cyberwar superpowers?. World Economic Forum. Retrieved From: https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers

Carrapico H., & Barrinha, A. (2017). The EU as a Coherent (Cyber)Security Actor?. Journal of Common Market Studies. Volume 55 (Issue 6). https://doi.org/10.1111/jcms.12575

Cirlig, C. (2014). Cyber defence in the EU. Preparing for cyber warfare?. European Parliamentary Research Service. Retrieved from https://epthinktank.eu/2014/10/31/cyber-defence-in-the-eu-preparing-for-cyber-warfare/

Council of the European Union (2019). COUNCIL DECISION concerning restrictive measures against cyber-attacks threatening the Union or its Member States. Retrieved from: http://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf

Council of the European Union (2019). Declaration by the High Representative on behalf of the EU on the alignment of certain third countries concerning restrictive measures against cyber-attacks threatening the Union or its member states. Retrieved from: https://www.consilium.europa.eu/en/press/press-releases/2019/07/02/declaration-by-the-high-representative-on-behalf-of-the-eu-on-the-alignment-of-certain-third-countries-concerning-restrictive-measures-against-cyber-attacks-threatening-the-union-or-its-member-states/

Council of the European Union (2019). Implementation of the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities – Attribution of malicious cyber activities – discussion of a revised text. Brussels, Belgium. Retrieved from: http://www.statewatch.org/news/2019/mar/eu-council-cyber-6852-REV-1-19.pdf

Council of the European Union. (2017). Cyber attacks: EU ready to respond with a range of measures, including sanctions. Retrieved from: https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

Council of the European Union. (2016). Non-paper: Developing a joint EU diplomatic response against coercive cyber operations – final revised text. Brussels, Belgium. Retrieved from: http://statewatch.org/news/2016/jul/eu-council-diplomatic-response-cyber-ops-5797-6-16.pdf

Deloitte (2020). Developing cybersecurity capabilities for the EU NIS Directive. Retrieved from: https://www2.deloitte.com/be/en/pages/risk/articles/Developing-cybersecurity-capabilities-for-EU-NIS-Directive.html

G7/8 Foreign Ministers Meetings. (2017). G7 Declaration on Responsible States Behavior in Cyberspace. Retrieved from: http://www.g8.utoronto.ca/foreign/170411-cyberspace.html

General Secretariat of the Council. (2017). Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") – Adoption. Retrieved from: http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

General Secretariat of the Council. (2015). Council Conclusions on Cyber Diplomacy. Retrieved from: http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf

Hill. C. (1993). The Capability-Expectations Gap, or Conceptualizing Europe's International Role. Journal of Common Market Studies. Volume 31 (Issue 3). https://doi.org/10.1111/j.1468-5965.1993.tb00466.x

Howorth, J. (2007). Security and Defence Policy in the European Union (2nd ed. 2014). Red Globe Press

Ivan, P. (2019). Responding to cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox. European Policy Centre. Retrieved from: https://epc.eu/en/publications/Responding-to-cyberattacks-EU-Cyber-Diplomacy-Toolbox~218414

Journal of the European Union. (2019). Council Regulation (EU) 2019/796 of 17 May 2019 Concerning restrictive measures against cyber-attacks threatening the Union or its Member State. Brussels, Belgium. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0796&from=EN. Last Access: 3rd January 2020

Missiroli, A., Dwan R., Economides, S., Pastore, F., Tonra, B. (2001). Coherence for Security Policy. Paris, France: Institute for Security Studies. Occasional Papers. Retrieved From: https://www.iss.europa.eu/sites/default/files/EUISSFiles/occ027.pdf

Moret, E., & Pawlak P. (2017). The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?. European Union Institute for Security Studies. DOI: 10.2815/399444

Munich Security Conference. (2019). More European, More Connected and More Capable. Building the European Armed Forces of the Future. Retrieved from: https://securityconference.org/en/news/full/more-european-more-connected-and-more-capable-msc-presents-new-report-on-european-defense-cooperation/

Nye, J.S. (2017). Deterrence and Dissuasion in Cyberspace. International Security. Volume 41 (Issue 3). https://doi.org/10.1162/ISEC_a_00266

Nye Jr, J.S. (2015). Can Cyber Warfare Be Deterred?. Project Syndicate. Retrieved from: https://www.project-syndicate.org/commentary/cyber-warfare-deterrence-by-joseph-s--nye-2015-12?barrier=accesspaylog

Politico (2018). EU Cyber Restrictive Measures: DK/EE/FI/LT/LV/NL/RO/UK non-paper. (2018). Retrieved from: https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2018/10/POLITICO-non-paper-cyber-sanctions-regime-OCT-10.pdf

Polyakova, A. & Boyer S. P. (2018). The Future Of Political Warfare: Russia, The West, And The Coming Age Of Global Digital Competition. Brookings. Retrieved from: https://www.brookings.edu/research/the-future-of-political-warfare-russia-the-west-and-the-coming-age-of-global-digital-competition/

Rugge, F. (2019). The Global Race For Technological Superiority. Milan, Italy: Ledizioni LediPublishing. Retrieved from: http://digital.casalini.it/9788855261456

Rugge, F. & Massolo, G. (2018). Confronting An "Axis Of Cyber"?, China, Iran, North Korea, Russia in Cyberspace. Milan, Italy: Ledizioni LediPublishing. Retrieved from: https://www.ispionline.it/sites/default/files/pubblicazioni/cyber_def_web2.pdf

Schelling, T. C. (1981). The Strategy of Conflict. Harvard University Press

Schmitt, M. N. (2013). 2013. The Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge, United Kingdom: Cambridge University Press. https://doi.org/10.1017/CBO9781139169288

Snyder, G. H. (1961). Deterrence and Defense: Toward a Theory of National Security. Princeton, New Jersey: Princeton University Press

World Economic Forum (2019). The Global Risks Report 2019. Retrieved from: https://www.weforum.org/reports/the-global-risks-report-2019