Dóra Dévai

The International Cyberspace Policy of the European Union

Introduction

By the 2010s, as cyberspace has become a scene for geopolitical contest, the need arouse in several areas for the European Union to take a more coherent and unified stance globally. The growing number of significant cybersecurity incidents prompted a mindset change from handling these as law enforcement or critical infrastructure technical issues. In the assessment of the European Commission looking back at that period:

> "As far as the national level of preparedness was concerned, Member States had very different level of capabilities and only a few Member States had adopted national cyber security strategies. The EU also had no diplomatic engagement with key partners on cyber issues with participation of Member States, cybersecurity was dealt with sporadically within sectorial dialogues."[1]

In response to this demand, the international cyberspace policy of the EU was established as one of the five strategic priorities of the 2013 Cybersecurity Strategy. Ever since then, this policy dimension gets increasingly integrated, or in EU jargon, mainstreamed into the existing External Action instruments of the Union. As a result, the international cyberspace policy is an umbrella term comprising a set of multifaceted areas aiming to promote wide-ranging EU political, economic and strategic interests.

The Global Context

The number of people using the Internet has grown exponentially, in particular in the developing countries where the online population is beyond 2.5 billion,

[1] European Commission: European Commission Working Staff Document SWD 295 final, 2017. 7–10.

https://doi.org/10.36250/01039_04

surpassing the 1 billion users in the developed world. The digital divide still exists: almost 78% of the people in Africa and 56% in the Asia-Pacific region are still offline. The growing importance of emerging or mid-income economies plays a growing role in generating Internet-linked wealth.[2] Digital questions are gathering an increased attention in the agendas of the African Union Commission and of African leaders. The group of digital giants have been joined by companies like the China-based e-commerce giant Alibaba or Tencent. Analyses show the increasing competitiveness of IT hubs like Beijing, Singapore, São Paolo, Moscow and Bangalore.[3]

In line with the immense role of digital data, data governance is a major preoccupation. Russia, for example, is moving towards a more digital sovereignty, requesting tech giants to store the data of Russian users on data centres in Russia. A new bill propositions the creation of Runet, a Russian Internet infrastructure that could operate independently of the rest of the Internet. Other countries are still looking for a strategy. In particular for small countries, international solutions remain the best way to protect their digital interests. At the same time, there is a very little appetite for multilateral solutions. 2019 was marked by major divisions.[4]

Internet Governance

In broad terms, Internet governance covers the technical, regulatory and policy issues concerning the infrastructure of the Internet and the data transmitted thereby. The list is ever extending, but some of the subject areas in focus are: artificial intelligence, data governance, digital inclusion and safety, security, stability and resilience. The Internet consists of the infrastructural and the logical layers. Some of the core elements of the infrastructure are, for example, the Internet backbone (IP networks), Internet exchange points, terrestrial and undersea cables, or communications satellites. The logical layer consists of root services, domain names, IP addresses, Internet protocols. These governance activities are embraced by a large number of international public and private organisations.

[2] Patryk Pawlak: Operational Guidance for the EU's International Cooperation on Cyber Capacity Building. *EUISS,* 31 August 2018.

[3] Ibid.

[4] DiploFoundation: *Diplo's Crystal Ball Exercise: Digital Policy in 2019.*

Table 1. *Some key Internet governance actors*

Infrastructure layer					
ITU International Telecommunication Union	*IEEE* Institute of Electrical and Electronics Engineers	*IETF* Internet Engineering Task Force	*Network Operator Groups*	*GSMA* Global System for Mobile Communications Association	*National ICT Ministers*
Logical layer					
ICANN Internet Corporation for Assigned Names and Numbers *IANA* Internet Assigned Numbers Authority	*ISO* International Organization for Standardization	*W3C* World Wide Web Consortium	*ISOC* Internet Society	*TLD* Operators Top-level domain	ETSI The European Telecommunications Standards Institute

Source: Compiled by the author based on Pawlak (2018): op. cit. 17.

Internet governance has high-stake cross-cutting effects, ranging from human rights to digital economy, and thus it is a highly contested area. This is well reflected by the long-standing debate on the different governance models prompted. The EU's standpoint was established in 2012 and updated in 2014 in the Council Conclusions on Internet Governance. From the onset of the debates, the EU has advocated that the Internet should be treated as a single unfragmented space. In order to achieve legitimacy, accessibility and transparency, a multi-stakeholder approach should be taken. This means an amalgam of non-state and state ownership and governance model, and inclusive bottom-up dialogue in decision-making. With the leadership of China and Russia at global forums, the opposing group often identified by the Shanghai Cooperation Organization and the MENA nations among others, is committed to a government-led Internet governance, exercising state control over ownership and content.

Cyberspace as a Diplomatic Field

The promotion of a rules-based international system is a core value of EU foreign and security policy. In this dimension, the main aim is to establish international

stability and conflict prevention in cyberspace via engagement with key international partners and organisations. The landmark event generally considered as a launching point was when in 1998 Russia brought on the agenda a draft resolution on *Developments in the Field of Information and Telecommunications in the Context of International Security* in the First Committee of the UN General Assembly advocating the regulation of the use of ICT tools for national security purposes. In 2004, the first UN Group of Governmental Experts (UN GGE) was convened to deliberate threats in the sphere of information security and possible cooperative measures to address them, hence, the UN GGEs have become the main source for the discussion about international security and stability in cyberspace based on three main pillars:

- The application of existing *international law* in cyberspace. Broadly speaking, there is a fragile consensus agreed in the 2013 UN GGE report that international law is applicable to maintain peace and stability in cyberspace. Nonetheless, there is a stark debate about how to implement the existing international law in cyberspace.
- *Norms of responsible state behaviour* in cyberspace. The same UN GGE report included 11 recommended norms and principles for responsible behaviour in cyberspace for the purposes of international security. Norms in international relations are based on the agreement between states, and thus shape the expectations of state behaviour in the international community. These are conditioned on mutual understanding, and are voluntary and non-binding.
- *Confidence-Building Measures (CBMs)* in cyberspace. Rooted in arms control regimes, these steps aim to build transparency, predictability and thus stability in order to restrain the use of force by reducing the causes of mistrust, misunderstanding and miscalculation between states. The UN GGE has developed a list of voluntary CBMs for cyberspace. These were then adopted at regional settings, most notably at the Organisation for Security and Cooperation in Europe. The OSCE adopted two sets of CBMs in 2013 and 2016.[5]

The EU in a strong cooperation with the U.S. has been at the forefront of the above diplomatic avenues. The list of norms, rules and principles of responsible

[5] Pawlak (2018): op. cit.

behaviour based on the UN GGE 2015 Report set the basis for the norms promoted collectively by the EU cyber diplomacy policy. For example:[6]

- States should not knowingly allow their territory to be used for internationally wrongful acts[7] using ICTs.
- States should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.
- States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts.

These were also refined in legal terms by an academic group of experts in so far that the most comprehensive resource is the Tallinn Manual 1.0 and 2.0 on the International Law of Cyber Operations.[8]

The other end of the spectrum is co-lead by Russia and China. Russia's *Information Security Doctrine,* adopted in 2016, acknowledges that universally recognised principles and norms of international law form the legal framework of the doctrine but does not include any specific reference to whether or not existing laws apply to cyberspace. Similarly, China's *International Strategy of Cooperation on Cyberspace,* released in 2015, merely contains a commitment to "study the application of international law in cyberspace from the perspective of maintaining international security, strategic mutual trust and preventing cyber conflicts".[9] Furthermore, both countries promote a new set of rules to govern cyberspace. The last GGE in 2016–2017 ended without being able to reach a consensus.

One of the most controversial international law concepts in the 2013 and 2015 UN GGE reports is that of sovereignty. States, mostly authoritarian that

[6] This listing has been edited by the author based on the *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* (A/70/174), 22 July 2015. 7–8.

[7] Rule 14 – Internationally wrongful cyber acts: 'A State bears international responsibility for a cyber-related act that is attributable to the State and that constitutes a breach of an international legal obligation.' (Michael N. Schmitt (ed.): *Tallinn Manual 2.0. on the International Law Applicable to Cyber Operations.* NATO Cooperative Cyber Defence Centre of Excellence, 2017. 84).

[8] Jochen Rehrl (ed.): *Handbook on Cybersecurity. The Common Security and Defence Policy of the European Union.* Luxembourg Publications Office of the European Union, 2018.

[9] Pawlak (2018): op. cit.

are concerned about exercising governmental control over their 'information space' generally interpret sovereignty as a right to be free from outside interference and influence. Liberal democracies deem such an understanding of sovereignty unacceptable as it is contrary to their commitment to human rights. For them, sovereignty as a foundational principle of international law entails sovereign equality, meaning that all are equal before the law.[10] The interpretation of sovereignty is far from being unified even among liberal democracies. The question whether sovereignty is a principle or a legal rule that places practical limits on the cyber activities of states has significant implications on the threshold at which offensive cyber activities violate international law. In the first case, the threshold will be relatively high: unless they constitute a prohibited intervention or use of force, they are likely to be held as lawful. Conversely, cyber operations below that threshold may nevertheless constitute a violation of sovereignty.[11] Other international law rules and principles, notably the rules regarding jurisdiction, the prohibition of intervention, and the obligation of due diligence are also derived from the principle of sovereignty.[12]

The EU's International Cyberspace Policy Framework

The watershed moment arrived with the Joint Communication entitled *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* The document laid down the principles, the statutory and institutional foundations of the policy. "Mainstreaming cyberspace issues into EU external relations and Common Foreign and Security Policy [CFSP]" entails that the same body of statutory and institutional rules and instruments apply to the EU's international cyberspace policy. The EU's stance on global cyberspace security and stability has been described above. The next section provides an overview of the major policy areas embraced by the EU's international cyberspace policy.

[10] Rehrl (2018): op. cit.; Schmitt (2017): op. cit.
[11] Rehrl (2018): op. cit.
[12] Ibid.

Human Rights and the Policy Principles

The EU often instrumentalises its normative authority, and one of the five key principles in the 2013 EU Cybersecurity Strategy is that the same laws apply in the cyber domain as in other areas of our daily lives. It should be stressed that cybersecurity is closely interlinked with human and fundamental rights, such as the rights to freedom of expression and the protection of personal data. The General Provisions on the Union's External Action also highlight human rights as a core value.

As a result, in 2014 the Foreign Affairs Council adopted *The EU Human Rights Guidelines on Freedom of Expression Online and Offline.* These principles facilitate building trust, and provide legitimacy and authority to the EU's international efforts. The two other principles in the Strategy are interrelated, too. Shared responsibility is a derivative of the multi-stakeholder Internet governance,[13] and emphasises the whole-of-government approach to cybersecurity.

Dialogue With Third Countries

The Strategy designates a number of External Action and CFSP areas to further align cybersecurity with the diplomatic domains. Most of these have been mentioned above. In addition, engaging in dialogue with third countries to build trust, reduce risks, promote information sharing and cooperation, and EU interests, a number of partnerships with third countries have been formalised. New regular policy dialogues on cyber issues got on their way with the technologically developed strategic partners and major emerging markets – the U.S., Japan, South Korea, India and China as well as with key international organisations.[14] Nevertheless, these dialogues deliver results at a varying degree.[15]

[13] "The EU recognizes that the interconnected and complex nature of cyberspace requires joint efforts by governments, private sector, civil society, technical community, users and academia to address the challenges faced and calls on these stakeholders to recognize and take their specific responsibilities to maintain an open, free, secure and stable cyberspace." *Council Conclusions on Malicious Cyber Activities.* Brussels, 16 April 2018.

[14] European Commission (2017): op. cit.

[15] Rehrl (2018): op. cit.

Cybersecurity Capacity Building and Development

The 2013 Strategy also addresses channelling cybersecurity capacity building systematically into development and neighbourhood policies. The document highlights that:

- Building resilient information infrastructures and the prevention of cyber threats can contribute to a safer global cyberspace.
- Capacity building can embrace different EU aid instruments including assisting the training of law enforcement, judicial and technical personnel to address cyber threats, as well as supporting the creation of relevant national policies, strategies and institutions in third countries on cybersecurity and resilient information infrastructures in third countries.[16]

The EU has become one of the main actors regarding cyber capacity building in third countries. A set of *Council Conclusions on EU External Cyber Capacity Building Guidelines* were adopted in June 2018.

The governance of this policy area is predominantly shared between the EEAS and the Commission. Within the Commission DG Connect, the Cybersecurity Technology and Capacity Building (Unit H.1) is playing a significant role in devising and implementing and synthesising these policy measures with other cybersecurity areas such as the investment in research and innovation, or the international cybersecurity cooperation and negotiation in general.

The EU has allocated a remarkable amount of funding for cyber capacity building in third countries. Under the Instrument contributing to Stability and Peace, the European Neighbourhood Instrument and the Instrument for Pre-accession Assistance the total allocation amounted to €21.5 million between 2014 and 2017.[17]

[16] High Representative of the European Union for Foreign Affairs and Security Policy: 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) 1 final.

[17] Antonio Missiroli (ed.): *The EU and the World: Players and Policies Post-Lisbon. A Handbook.* European Union Institute for Security Studies, 2016.

The EU is mainly represented at these discussions by the Commission, for example, the Next-Generation Internet (Unit E.3) within the Commission's DG Connect.

> "The Unit is the centre of competence for Next Generation Internet focussing on novel technological breakthroughs, new architectural solutions and advanced service concepts. It also ensures the EU vision and voice on Internet Governance in fora such as IGF, ICANN, G8, ITU and WSIS (DG Connect)."[18]

The EU's overall Internet strategy is set by two Council Conclusions on Internet Governance (2012, 2014) whereby the EU supports a multi-stakeholder governance model of the Internet that is based on clear principles, in line with the "Netmundial" principles endorsed by EU Member States.[19]

The Cyberspace Diplomacy of the EU

Pursuant to the institutional setting of the EU's External Actions and CFSP, the main political decision-making and legislative power for cyberspace diplomacy rests with the Member States through the Council of the EU. The Commission and the High Representative (HR) of the European External Action Service are responsible for the development of strategies, policies and draft legislation, as well as for their execution.

Within the Security Policy Directorate (SECPOL) of the EEAS there is a cyber sector responsible for the formulation, implementation and coordination of cybersecurity and defence issues under the Common Foreign and Security Policy. The SECPOL is actively engaged in the multilateral diplomatic activities.[20]

The European Commission helps to shape the EU's overall strategy, proposes new EU laws and policies, monitors their implementation and manages the EU budget. Along the HR and the Member States, the Commission actively engages in policy dialogue with international partners and with global, regional, sectoral and specialised international organisations.

[18] Dg Connect Next-Generation Internet (Unit E.3): *Shaping Europe's Digital Future.* 2016.
[19] European Commission (2017): op. cit.
[20] Rehrl (2018): op. cit.

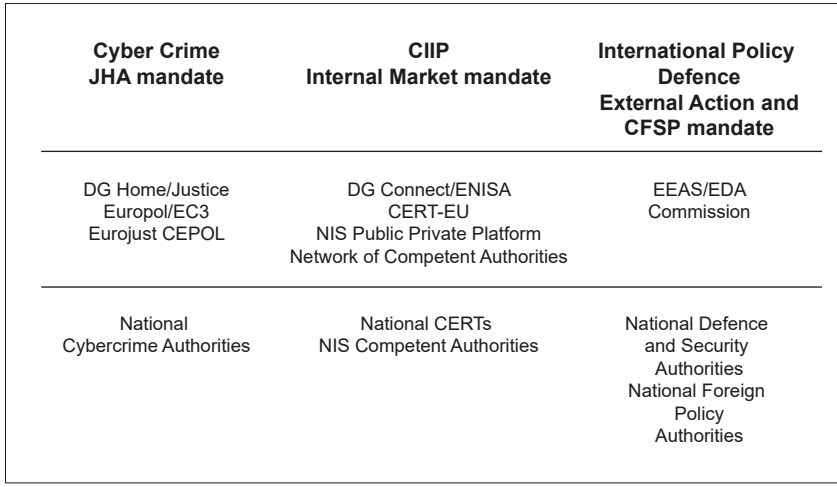

Figure 1. *The main pillars of the EU Cybersecurity Strategy*
Source: Christou (2016): op. cit.

The Changing Cybersecurity Threat Landscape and the EU's Strategy Development

By 2015, at the global and regional fora, cyber diplomatic negotiations came to a second round, and the Russian military intervention in Ukraine reshaped security thinking in Europe. The EU had endorsed a number of new security policy documents. The *Council Conclusions on Cyber Diplomacy,* adopted in February 2015, catalogued and consolidated the cyber diplomacy objectives of the 2013 Strategy.

The threat landscape has also evolved significantly in the period between 2015 and 2017: disruptive cyber operations against critical infrastructures in Ukraine; the midterm elections meddling in the U.S.; massive botnet attacks and global ransomware cases like 'WannaCry' and 'NotPetya' shaped the political climate. Moreover, ICANN was freed from U.S. government oversight. Six EU Member States were engaged in the 2016–2017 UN GGE work – the United Kingdom, France, Germany, Estonia, the Netherlands, Finland – which came to an end without being able to establish a consensus report.

Consequently, the EU's approach was altered. The 2012 *Communication on the EU Strategic Approach to Resilience* defines resilience as 'the ability of an

individual, a household, a community, a country or a region to withstand, adapt and quickly recover from stress and shocks'.[21] The EU's approach to cybersecurity issues shifted from crisis containment to a more structural and long-term approach to vulnerabilities, with an emphasis on anticipation, prevention and preparedness.[22] The Joint Communication on *A Strategic Approach to Resilience in the EU's External Action* adopted in 2017 also marked this new direction.

In 2017, a progress report was conducted on the achievements of the 2013 Strategy. The Commission recognised that many of the objectives "were defined in very general terms, showing the direction the EU should follow. Therefore, the assessment looks at the degree of progress made without the assumption that the objective could have been fully met".[23] In September 2017, the HR and the Council's Joint Communication on *Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU* was endorsed as a result. The document aims at creating a more coherent policy framework by:

- building EU resilience to cyberattacks through the instalment of established institutional procedures, such as the *Blueprint* for EU-wide cyber crisis management
- creating effective cyber deterrence in particular through the *Cyber Diplomacy Toolbox*[24]

A turning point came in the first half of 2016, when the Dutch EU presidency circulated a non-paper among Member States on the concept of coordinated response to coercive cyberattacks. The document defined coercive cyberattacks as 'cyber operations that constitute an internationally wrongful act intended to exert undue diplomatic, informational, military or economic pressure on a target State'.[25] State and nonstate actors carry out such operations for politico–military purposes on the basis of a rational cost/benefit analysis. Therefore, cyber diplomacy is one of the tools to influence this analysis by increasing the costs of coercive cyber operations and establishing a deterrent effect. The non-paper

[21] European Commission: Communication from the Commission to the European Parliament and the Council. The EU Approach to Resilience: Learning from Food Security Crises. COM(2012) 586 final.

[22] Pawlak (2018): op. cit.

[23] European Commission (2017): op. cit. 53.

[24] Pawlak (2018): op. cit.

[25] Presidency of the European Council: Non-paper: Developing a Joint EU Diplomatic Response against Coercive Cyber Operations. 5797/4/16 REV 4, 2016. 4.

also emphasised that unlike the earlier cyber diplomacy concepts which aimed at increasing global cybersecurity in general, the optional diplomatic measures suggested in this non-paper are intended to respond to specific incidents threatening the security of the EU and its citizens and territory.[26]

Cyber Diplomacy Toolbox

The *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")* was endorsed in June 2017. The Council Conclusion affirms that malicious cyber activities might constitute wrongful acts under international law.[27] Up to this point, the EU treated 'cyber activities against information systems' and joint investigation and prosecution response mechanism under criminal law.[28] This time, the Conclusion "affirms that the existing measures within the Common Foreign and Security Policy, including, if necessary, restrictive measures, adopted under the relevant provisions of the Treaties, are suitable for a Framework for a joint EU diplomatic response to malicious cyber activities". Furthermore, the document premises that signalling the likely consequences of such malicious cyber activities influences the long-term behaviour of potential aggressors.[29]

Wrongful acts by a state are based on the customary international law of State responsibility and refer to the breaches of international law obligations of states.[30] What constitutes a malicious cyber activity and how to respond to them are highly contentious and politicised subjects in cyber diplomacy debates.[31] Based on the Tallinn Manual 2.0, the responsive measures can range from retorsion to self-defence. Retorsion is the "taking of measures that are lawful, albeit 'unfriendly'."[32] States have the right to apply retorsion, even when the origi-

[26] Ibid. 3.

[27] The Council of the European Union: Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") 9916/17, 2017.

[28] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks against Information Systems. The Directive contains minimum rules on the definition of criminal offences and sanctions in the area of attacks against information systems and provides for operational measures thus facilitating cross-border cooperation by law enforcement authorities.

[29] 2017/9916/ Council Conclusion.

[30] Schmitt (2017): op. cit. 84.

[31] Rehrl (2018): op. cit.

[32] Schmitt (2017): op. cit. 112.

nal malicious cyber activity does not reach the threshold of an internationally wrongful act or cannot be attributed to another state.[33] Countermeasures would otherwise be unlawful, but they are permissible if undertaken in response to another state's unlawful conduct. However, the original malicious cyber activity has to be attributed to a state, not merely to a non-state actor operating from the state's territory.[34] According to Article 51 of the UN Charter, a state's right to self-defence arises in the cyber context when a hostile cyber operation amounts to an 'armed attack'. In case of a cyber armed attack, the state is permitted to resort to force, including cyber operations at the 'use of force' level, to defend itself. Most 'Western powers' share in the understanding that certain malicious cyber operations may amount to the use of force or armed attack, and that it has a deterrent effect.[35]

After following the Draft Conclusions for months, the *Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities* was presented by the EEAS and the Commission containing the details of the Toolbox.[36] The guidelines provide a broad set of conditions under which the collective response measures can be applied: for example, they can be used 'to prevent or respond to a malicious cyber activity, including in case of malicious cyber activities that do not rise to the level of internationally wrongful acts but are considered as unfriendly acts'; they have to be based on shared situational awareness agreed among Member States. The scope of the perpetrators is not restricted to states, however, the document focuses primarily on state responsibility.

The CFSP instruments[37] that have been partially discussed above, for instance, international dialogue, or confidence and capacity building measures, provide the pool of collective diplomatic response measures. Response measures in this Framework are organised in five categories: Preventive measures; Cooperative measures; Stability measures; Restrictive measures; Possible EU

[33] Katriina Härmä – Tomáš Minárik: *European Union Equipping Itself against Cyber Attacks with the Help of Cyber Diplomacy Toolbox.* NATO Cooperative Cyber Defence Centre of Excellence, 2017.

[34] Ibid.

[35] Rehrl (2018): op. cit.

[36] The Council of the European Union: Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities. 13007/2017.

[37] The legal basis for the CFSP was set out in the TEU and revised in the Lisbon Treaty Title V, Articles 21–46.

support to Member States' lawful responses. Under the process to invoke the measures within the framework, the two CFSP crises management mechanisms can be mobilised as well: the Integrated Political Crisis Response (IPCR), and the invocation of the solidarity clause (Article 222 TFEU).

Attribution is a pivotal issue in response mechanisms. According to the guidelines:

> "Attribution of a malicious cyber activity remains a sovereign political decision based on all-source intelligence, taken on a case-by-case basis. Every Member State is free to make its own determination with respect to attribution of a malicious cyber activity."[38]

> "Not all of the measures presented in this Framework will require attribution: they are a means of preventing or resolving a cyber incident, expressing concerns and signalling them in another way. Furthermore, the use of the measures within the Framework can be tailored to the degree of certainty that can be established in any particular case."[39]

Cybersecurity Attribution

In order to fully comprehend the evolution of the EU's international cybersecurity policy, and especially the Cyber Diplomacy Toolbox, the problems stemming from the attribution need to be surveyed systematically. In the cybersecurity context, the so-called attribution problem is one of the most difficult technical hurdles to overcome. Moreover, attribution is also at the core of the response measures at the political and strategic level. In March 2019, the EEAS presented a non-paper on the *Implementation of the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities – Attribution of Malicious Cyber Activities* that defines attribution 'as a practice of assigning responsibility for a malicious cyber activity to a specific actor'.[40] The problem arises from the fact that there is no standardised agreement on how to achieve reliable attribution at the technical or the political level. Moreover, the technical, human and political attribution all have significant barriers. On the other hand, those deficiencies offer plausible deniability for cyberspace perpetrators.

[38] The Council of the European Union: 13007/2017.

[39] Ibid.

[40] European External Action Service (EEAS): Implementation of the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities – Attribution of Malicious Cyber Activities. 6852/1/19, 2019. 2.

First, it is essential to consider the different attribution layers. One prominent academic researcher, Thomas Rid, for example, differentiates between three levels of attribution:

> "The tactical goal is understanding the incident primarily in its technical aspects, the how. The operational goal is understanding the attack's high-level architecture and the attacker's profile the what. The strategic goal is understanding who is responsible for the attack, assessing the attack's rationale, significance, appropriate response the who and why. Finally, communication is also a goal on its own: communicating the outcome of a labour-intensive forensic investigation is part and parcel of the attribution process, and should not be treated as low priority."[41]

Technical attribution consists of analysing malevolent functionality and malicious packets, and using the results of the analysis to locate the node which initiated, or is controlling the attack.[42] Next, what Rid classified as the operational layer of the attribution process strives to synthesise all-source intelligence. Analysts functioning on the operational layer develop competing hypotheses to explain the incident. However, the uncertainty of attributive statements is likely to increase as the analysis moves from technical to political, including the question of the attacker's motivation.[43]

On a strategic level, leaders and top analysts are tasked with aggregating the answers to operational questions, such as intelligence gain/loss, in order to draw meaningful conclusions. Finally, political leaders have to decide about the optimal response measure involving the dilemma of public attribution that best suits the state's interest in the given situation, as well as on a strategic time scale.

According to the EU non-paper *Implementation of the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities – Attribution of Malicious Cyber Activities:*

> "Coordinated attribution could signal strong EU Member States' capabilities to establish with certainty that an actor holds responsibility for a malicious cyber activity could be also taken into account, as it can diminish an actor's willingness and ability to carry out further malicious activities."[44]

[41] Thomas Rid – Ben Buchanan: Attributing Cyber Attacks. *Journal of Strategic Studies,* 38, nos. 1–2 (2014). 4.

[42] W. Earl Boebert: A Survey of Challenges in Attribution. In *Proceedings of a Workshop on Deterring Cyberattacks. Informing Strategies and Developing Options for U.S. Policy.* Washington, D.C., The National Academies Press, 2010.

[43] Rid–Buchanan (2014): op. cit.

[44] EEAS: 6852/1/19, 2019. 4.

Coordinated attribution have come to the forefront of recent political and diplomatic discussions. Based on the precedent set over the past years, some nation states have increasingly resorted to public attribution as an important diplomatic asset of their cyberattack response strategy, which also means that they become more willing to overcome information sharing barriers to achieve shared situational awareness. For instance, in December 2017, the Five Eye countries, the U.K., the USA, Canada, Australia and New Zealand have often joined to call out cyberattacks that have been attributed to nation states, among others, pointing the finger at North Korea for WannaCry. In February 2018, the U.K. and Denmark, together with the USA and Australia, publicly attributed the NotPetya cyberattack to the Russian Government. In these collective actions there is also the intention of setting norms of what is not acceptable state behaviour in cyberspace, and thus signalling that it will have repercussions.

So far, some of the joint public EU response measures to malicious cyber activity are:

- declaration by the High Representative on behalf of the EU condemning the cyberattack against Georgia (February 2020)
- declaration by the High Representative on behalf of the EU stressing the need to respect the rules-based order in cyberspace (April 2019)
- statement by Commission President Juncker, High Representative Mogherini and Council President Tusk on the targeted cyberattack against OPCW (October 2018)
- Council Conclusions responding to malicious cyber activities, including WannaCry and NotPetya (April 2018)

EU Cyber Sanctions

On 17 May 2019, the Council of the European Union adopted *Council Decision Concerning Restrictive Measures against Cyber-attacks Threatening the Union or its Member States*[45] and the *Council Regulation Concerning Restrictive Measures against Cyber-attacks Threatening the Union or its Member States.*[46]

[45] The Council of the European Union: Council Decision (CFSP) 2019/797 of 17 May 2019 Concerning Restrictive Measures against Cyber-attacks Threatening the Union or its Member States.
[46] The Council of the European Union: Council Regulation (EU) 2019/796 of 17 May 2019 Concerning Restrictive Measures against Cyber-attacks Threatening the Union or its Member States.

The new legislation was a follow-up on the Conclusions establishing the Cyber Diplomacy Toolbox. The Council Decision and Regulation constitute a remarkable step forward in the line of thought on responsive measures to cyberattacks. Before, the EU could impose sanctions only on persons and entities involved either in terrorism, or in the proliferation of chemical weapons. Consequently, it is essential to have a legislation that specifically tackles cyberspace-related threats.

A cyber activity for consideration here means an action that includes: access to information systems; information system interference; data interference; or data interception. Sanctions can be imposed on planned attacks as well. To be subject to sanctions, a cyberattack must fulfil two criteria: the attack has a significant effect; and the attack constitutes an external threat to the Union or its Member States. When deliberating whether a cyberattack has a significant effect, a series of indicators are to be considered: the scope, scale, impact or severity of disruption caused; the number of natural or legal persons, entities or bodies affected; the number of Member States concerned; the amount of economic loss caused; the economic benefit gained by the perpetrator, for themselves or for others; the amount or nature of data stolen or the scale of data breaches; and the nature of commercially sensitive data accessed.[47] The ruling only applies to external cyberattack targets against an EU institution, Member State. In addition, when it is necessary to achieve an EU common security and defence policy objective, sanctions can also be imposed as a response to cyberattacks with a significant effect against third States or international organisations. Sanctions can materialise essentially in two ways: a prevention of the entry of the sanctioned into, or transit through, territories of EU Member States; second, no funds or economic resources shall be made available directly or indirectly to or for the benefit of the listed.

In sharp contrast to the legislation's antecedents, namely the 2017 *Conclusion on the Toolbox, its Implementing Guidelines and the Non-paper on Attribution,* the sanctions can be directed only against natural or legal persons, other entities or bodies different from a State. Focusing on individually listed non-State actors, the sanctions are targeted or 'smart', i.e. intended to harm a precisely defined subject which represents a threat, not to affect a whole State and its population.[48]

[47] Adam Botek: *European Union Establishes a Sanction Regime for Cyber-attacks.* NATO Cooperative Cyber Defence Centre of Excellence, 2019.
[48] Ibid.

On 30 July 2020, the first ever sanctions were imposed by the Council against six individuals and three entities responsible for or involved in various cyber-attacks. These include the attempted cyberattack against the OPCW (Organisation for the Prohibition of Chemical Weapons) and those publicly known as "WannaCry", "NotPetya" and "Operation Cloud Hopper".

The sanctions imposed include a travel ban and an asset freeze. In addition, EU persons and entities are forbidden from making funds available to those listed.

The Way Forward: The EU's Cybersecurity Strategy for the Digital Decade

Table 2. *Strategic initiatives related to the international cyberspace policy in the EU's Cybersecurity Strategy for the Digital Decade*

Pillar 2	Pillar 3
Encourage and facilitate the establishment of a Member States' cyber intelligence working group residing within the EU INTCEN Advance the EU's cyber deterrence posture to prevent, discourage, deter and respond to malicious cyber activities	Advance international security and stability in cyberspace, notably through the proposal by the EU and its Member States for a Programme of Action to Advance Responsible State Behaviour in Cyberspace (PoA) in the United Nations Offer practical guidance on the application of human rights and fundamental freedoms in cyberspace Expand EU cyber dialogue with third countries, regional and international organisations, including through an informal EU Cyber Diplomacy Network Reinforce the exchanges with the multi-stakeholder community, notably by regular and structured exchanges with the private sector, academia and civil society Propose an EU External Cyber Capacity Building Agenda and an EU Cyber Capacity Building Board

Source: Compiled by the author based on European Commission (2020): op. cit.

The new EU Cybersecurity Strategy seeks to tackle the evolving threat landscape in a complex manner. The strategy contains concrete proposals for deploying three principal instruments – regulatory, investment and policy instruments –

to address three areas of EU action: (1) resilience, technological sovereignty and leadership; (2) building operational capacity to prevent, deter and respond; and (3) advancing a global and open cyberspace.[49] In terms of the Cyber Diplomacy Toolbox, the strategic initiatives shown in Table 2 are designated for action.

References

Boebert, W. Earl: A Survey of Challenges in Attribution. In *Proceedings of a Workshop on Deterring Cyberattacks. Informing Strategies and Developing Options for U.S. Policy.* Washington, D.C., The National Academies Press, 2010. Online: https://doi.org/10.17226/12997

Botek, Adam: *European Union Establishes a Sanction Regime for Cyber-attacks.* NATO Cooperative Cyber Defence Centre of Excellence, 2019.

Christou, George: *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy.* London, Palgrave Macmillan, 2016. Online: https://doi.org/10.1057/9781137400529

Dg Connect Next-Generation Internet (Unit E.3): *Shaping Europe's Digital Future.* 2016.

DiploFoundation: *Diplo's Crystal Ball Exercise: Digital Policy in 2019.* Online: https://etradeforall.org/news/diplos-crystal-ball-exercise-digital-policy-in-2019-10-areas-of-development-which-we-will-need-to-watch-closely/

European External Action Service (EEAS): Implementation of the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities – Attribution of Malicious Cyber Activities. 6852/1/19, 2019.

EU Cyber Direct: Council Conclusions on Cyber Diplomacy. 2019.

European Commission: Communication from the Commission to the European Parliament and the Council. The EU Approach to Resilience: Learning from Food Security Crises. COM(2012) 586 final.

European Commission: Working Staff Document SWD 295 final, 2017.

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

EU INCENT Fact Sheet: The EU Intelligence Analysis Centre. 2015.

Härmä, Katriina – Tomáš Minárik: *European Union Equipping Itself against Cyber Attacks with the Help of Cyber Diplomacy Toolbox.* NATO Cooperative Cyber Defence Centre of Excellence, 2017.

High Representative of the European Union for Foreign Affairs and Security Policy: 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) 1 final.

Missiroli, Antonio (ed.): *The EU and the World: Players and Policies Post-Lisbon. A Handbook.* European Union Institute for Security Studies, 2016.

[49] European Commission: Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade. JOIN (2020) 18 final. 4.

Pawlak, Patryk: Operational Guidance for the EU's International Cooperation on Cyber Capacity Building. *EUISS,* 31 August 2018.
Presidency of the European Council: Non-paper: Developing a Joint EU Diplomatic Response against Coercive Cyber Operations. 5797/4/16 REV 4, 2016.
The Council of the European Union: Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") 9916/17, 2017.
The Council of the European Union: Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities. 13007/2017.
The Council of the European Union: Council Decision (CFSP) 2019/797 of 17 May 2019 Concerning Restrictive Measures against Cyber-attacks Threatening the Union or its Member States.
The Council of the European Union: Council Regulation (EU) 2019/796 of 17 May 2019 Concerning Restrictive Measures against Cyber-attacks Threatening the Union or its Member States.
The Council of the European Union: EU Imposes the First Ever Sanctions against Cyber-attacks. *Press Release,* 30 July 2020.
Rid, Thomas – Ben Buchanan: Attributing Cyber Attacks. *Journal of Strategic Studies,* 38, nos. 1–2 (2015). 4–37. Online: https://doi.org/10.1080/01402390.2014.977382
Rehrl, Jochen (ed.): *Handbook on Cybersecurity. The Common Security and Defence Policy of the European Union.* Luxembourg Publications Office of the European Union, 2018. Online: https://doi.org/10.2855/3180
Schmitt, Michael N. (ed.): *Tallinn Manual 2.0. on the International Law Applicable to Cyber Operations.* NATO Cooperative Cyber Defence Centre of Excellence, 2017.
United Nations Group of Governmental Experts: *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* (A/70/174), 22 July 2015.