Cyber Diplomacy from the European Perspective

Edited by
Anna Molnár and Balázs Mártonffy

LUDOVIKA
UNIVERSITY PRESS

Cyber Diplomacy
from the European Perspective

Cyber Diplomacy from the European Perspective

Edited by
Anna Molnár and Balázs Mártonffy

LUDOVIKA
UNIVERSITY PRESS
Budapest, 2022

Authors
Dóra Dévai
Csaba Krasznay
Balázs Mártonffy
Anna Molnár
Dóra Molnár
Anita Tikos

Consultant
Zoltán Szenes

Published by the Universitiy of Public Service
Ludovika University Press
Responsible for publishing: Gergely Deli, Rector

Address: HU-1083 Budapest, Ludovika tér 2.
Contact: kiadvanyok@uni-nke.hu

Managing editor: Zsolt Kilián
Copy editor: Zsuzsánna Gergely
Layout editor: Zsolt Kilián

Printed and bound in Hungary.

DOI: https://doi.org/10.36250/01039_00

ISBN 978-963-531-827-8 (print)
ISBN 978-963-531-828-5 (ePDF)
ISBN 978-963-531-829-2 (ePub)

Contents

Balázs Mártonffy[1]

Cyber Diplomacy: A Review from the Literature

An Introduction to the Cyber World Amid the Covid-19 Pandemic

In 2013, the U.S. Department of Defense alone, one of the institutions that is most active in the cyber realm, reported 10 million efforts at intrusion each day.[2] Five short years later, in 2018, this figure was 36 million.[3] The numbers in the cyber realm do not stay constant for long; the cyber world changes extremely quickly. Thus, it will come as no surprise that any text on an issue as complicated and quickly changing as the cyber domain is bound to be outdated quickly. This review from the literature on cyber diplomacy, despite all efforts, is particularly prone to be overtaken by events as our society undergoes and fights the implications of the global pandemic of the early 2020s, the novel coronavirus that began in Wuhan, China, in late December 2019. Further, as this review work is written during the time that European Union member states fight the coronavirus and enter into force restrictions on movement, universities have undergone work-from-home transitions, this work relies fundamentally on literature that was available online when the research for this chapter was written. The irony of course, for a text on cyber diplomacy, is not lost on the author.

In the 21st century, the question of how much our society changes continues to linger. As mentioned above, this chapter is written during the global pandemic caused by the virus Sars-Cov-2 and the associated disease, Covid-19. The results and implications of this truly global crisis cannot be understated, and in April 2021, when this chapter is concluded, much remains to be determined. What we do know is that the effects will reverberate deeply through what has become a widely interdependent and truly globalised society across our globe by 2020.

[1] The author would like to thank Anna Urbanovics, PhD student at the University of Public Service, for her excellent research assistance.

[2] Brian Fung: How Many Cyberattacks Hit the United States Last Year? *Nextgov,* 08 March 2013.

[3] Frank R. Konkel: Pentagon Thwarts 36 Million Email Breach Attempts Daily. *Nextgov,* 11 January 2018.

https://doi.org/10.36250/01039_01

Of course, connecting cyber threat and global pandemics is not impossible: case in point is the 2018 study on the countermeasures available to protect critical healthcare infrastructure.[4] The study concluded that, if for example a pandemic like Covid-19 were to be compounded with an insider attack on a state's critical healthcare infrastructure, the results would be devastating.[5] Inasmuch as our current awareness of the implications of the virus's origins presumes to endeavour to analyse, this is not the case for the novel coronavirus, but certain conclusions must be drawn. Health care systems globally are under strain, and coupled with a kinetic or cyber-kinetic attack, the system could have been seriously upset. The transatlantic regions prime politico-military alliance, NATO, is also concerned: its Secretary General, Jens Stoltenberg, continues to state that the prime directive of the Alliance is to make sure that the public health crisis does not become a security crisis.[6]

This chapter serves to provide the reader with a general introduction into the world of cybersecurity and cyber diplomacy. The latter is a somewhat novel term that has been seen employed rarely in academic texts but is somewhat more prevalent in popular and media punditry. The specific goal of this chapter is to provide the reader with a conceptual understanding of what, as to the best of social scientific knowledge, cyber diplomacy is, and how it is being used in general language and in policy as well.

To begin with, let us examine some of the key terms that are needed to grapple with cyber diplomacy. For general considerations when thinking about issues in the cyber world and specifically about cyber diplomacy, I turn to Joseph S. Nye, Professor at Harvard University, who writes the following:

> "Cyber is a prefix standing for computer and electromagnetic spectrum-related activities. The cyber domain includes the Internet of networked computers but also intranets, cellular technologies, fiber-optic cables, and space-based communications. Cyberspace has a physical infrastructure layer that follows the economic laws of rival resources and the political laws of sovereign jurisdiction and control. This aspect of the Internet is not a traditional 'commons.' It also has a virtual or informational layer with increasing economic returns to scale and political practices that make jurisdictional control difficult. Attacks from the

[4] Steven Walker-Roberts – Mohammad Hammoudeh – Ali Dehghantana: A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure. *IEEE Access,* 6 (2018). 25167–25177.

[5] Ibid.

[6] North Atlantic Treaty Organization: *Press Conference by NATO Secretary General Jens Stoltenberg Following the Meeting of NATO Ministers of Foreign Affairs.* 02 April 2020.

> informational realm, where costs are low, can be launched against the physical domain, where resources are scarce and expensive. Conversely, control of the physical layer can have both territorial and extraterritorial effects on the informational layer. Cyber power can produce preferred outcomes within cyberspace or in other domains outside cyberspace."[7]

Cyber as the reader is undoubtedly well aware refers broadly speaking to the culture of computers, information technology and virtual reality. But the term is at times used interchangeably with 'e', virtual and digital. The specific etymology of the word cyber is also interesting. Why did we settle on cyber instead of virtual or electronic or digital? How do the terms interrelate? Here is what is commonly accepted on the terms etymology and how to differentiate between cyber, 'e', virtual and digital.

The etymology of 'cyber' goes back to the ancient Greek meaning of 'governing'. Cyber came to our time via Norbert Weiner's book *Cybernetics* and William Gibson's science-fiction novel *Neuromancer.* The growth in the use of the prefix 'cyber' followed the growth of the Internet. Today, cyber mainly refers to security issues; e- is the preferred prefix for economic issues, digital is mostly used by the government sector, while virtual has been practically abandoned.

'E' is the abbreviation for 'electronic'. It got its first use through e-commerce, as a description of the early commercialisation of the Internet. In the EU's Lisbon Agenda (2000) and the WSIS declarations (Geneva 2003; Tunis 2005), e- was the most frequently used prefix.[8] The WSIS follow-up implementation is centred on action lines including e-government, e-business, e-learning, e-health, e-employment, e-agriculture, and e-science. Nonetheless, e- is not as present as it used to be. Even the EU recently abandoned e-, trying, most likely, to distance itself from the failure of its Lisbon Agenda.

Digital refers to '1' and '0' – two digits that are the basis of the whole Internet world. In the past, digital was used mainly in development circles to represent the digital divide. During the last few years, digital has started conquering the Internet linguistic space, especially in the language and strategy of the European Union. Virtual relates to the intangible nature of the Internet.

Virtual reality could be both an intangible reality, (something that cannot be touched) and a reality that does not exist (a false reality). Academics and Internet pioneers used virtual to highlight the novelty of the Internet, and the

[7] Joseph S. Nye, Jr.: Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly,* 5, no. 4 (2011a). 19.

[8] World Summit on the Information Society: *Declaration of Principles.* 12 December 2003.

emergence of 'a brave new world'. Virtual, because of its ambiguous meaning, rarely appears in policy language and international documents.[9]

Cyber is thus the broadest category and the most useful one when it comes to conceptualising diplomacy. The term cyber diplomacy itself refers to diplomacy, and a specific form thereof and thus subpart thereof, diplomacy in the cyber realm. Diplomacy as a term is widely accredited to be a practice of states, and the easiest way to begin grappling with the term is to start there. Thus, cyber diplomacy at its core is simply diplomacy conducted in the cyber realm. Cyber diplomacy is both much larger then this simple definition and has much smaller integral parts. As I demonstrate later, one key differentiation that has to be made is that cyber diplomacy is a separate concept from digital or e-diplomacy, but digital diplomacy and e-diplomacy are used interchangeably. But why is diplomacy in the cyber realm different then in the traditional world? Let us examine in brief how it functions in the non-cyber realm.

States, as sovereign entities with a defined population and territory, territorial integrity, and external and internal legitimacy with some form or type of authority that holds the monopoly on the legitimate use of violence, have been a central actor in international relations theory. The modern state's emergence is attributed to the Peace of Westphalia, where the feudal system of overlapping realms of authority were channelled into hierarchical entities, with founts of authority resting with the state as an actor. Diplomacy, the profession, activity, or skill of managing international relations typically by a country's representatives abroad now was without question the mandate of states.

Diplomacy thus can be understood to be grouped into two large buckets. The first bucket is that of the specific, the note verbales, the demarches, the embassies, consulate, Ambassadors Extraordinary and Plenipotentiaries, Agréments, and other instances when states interact with each other. This is usually on two separate levels in our modern world: bilaterally, i.e. for example the deputy chief of mission of France to the Court of St. James delivers a demarche to the State Secretary of the Foreign and Commonwealth Office in London, the United Kingdom. But another type of fora is the multilateral realm, when states interact, usually as equals, in intergovernmental organisations such as the United Nations, or the World Health Organization.

The more general idea of diplomacy of course is what Kissinger in his world-famous book explores (aptly named Diplomacy) – the broadly understood conduct of states as actors in an international system, the manner in which they define their own national interest and the general way they carry these out.

[9] Jovan Kurbalija: *An Introduction to Internet Governance.* Msida–Geneva, DiploFoundation, 2016.

In this approach, diplomacy is one tool in the grand strategy toolkit of states to "get what they want". Usually separated from war, which is the "ultima ratio regum" as the cannons of Louis XIV had epitomised, diplomacy then is a term that relates to the use of power without active violence.

Cyber diplomacy can be defined as "an attempt to facilitate communication, negotiate agreements, gather intelligence and information from other countries to avoid friction in cyberspace, bearing in mind the foreign policy agenda".[10] It is important to note that while

> "in many articles, cyber-diplomacy is considered to be same as e-diplomacy or digital diplomacy. However, these concepts differ from each other. While cyber-diplomacy involves managing foreign policy in today's age, e-diplomacy or digital diplomacy reflects on the impact of new technology on the objective, tools, and structure of diplomacy. Digital diplomacy or e-diplomacy is the study of the use of ICT tools and method for diplomacy and foreign affairs. However, cyber-diplomacy involves diplomacy, conflict resolution, agreements and policies that is surrounding cyberspace."[11]

This divide is the most important differentiation, to know when to refer to cyber diplomacy in practice, that is instances of diplomacy conducted through cyber means as digital diplomacy (which is also called e-diplomacy) and when to refer to cyber diplomacy proper when it is the conduct of diplomacy that affects the cyberspace domain.

The difference between e/digital diplomacy and cyber diplomacy is visible in the U.S. academic language and if not quite so clearly elaborated, in European academia as well. For example, Mureşan's study on the "Current Approaches of Diplomacy in the Cyberspace" clearly recognises the need for cyber diplomacy.[12] Mureşan argues that

> "more and more frequently, the Internet has also been the target of many cyber attacks, generating data leaks and financial loses. The vast majority of financial and telecommunication systems have been affected by numerous such intrusions. These incidents are more and more common and they impact heavily both on governments and businesses or individual users."[13]

But here the digital and the cyber realms of diplomacy are still conflated.

[10] Cyber Peace Alliance: *Cyber Diplomacy: Governance Beyond Government.* 12 October 2019.
[11] Ibid.
[12] Mureşan Radu Constantin: Current Approaches of Diplomacy in the Cyberspace. *Studia Universitatis Babeş-Bolyai,* 62, no. 2 (2017). 31–44.
[13] Ibid. 31.

Illustrating the Differences Between Cyber Diplomacy and Digital Diplomacy

To illustrate with a concrete example the difference between the two major conceptual buckets of the term, let us take a recent example of cyber diplomacy and e-diplomacy or digital diplomacy.[14] The North Atlantic Treaty Organization, NATO, makes decisions as set forth in its charter, the Washington Treaty of 1949, by convening senior leaders of the Alliance in a room to approve certain documents that task the alliance to carry forth certain actions. The Foreign Ministers meet in addition to other times every spring. But the Covid-19 crisis did not allow for this to take place, as all NATO member states restricted travel out, and the usual host nation of the meeting, Belgium, where NATO's Headquarters are located in Brussels, did not allow non-nationals to visit. So the meeting was held via secured video teleconference, with the NATO Secretary General in Brussels, while the foreign ministers of the 30 member states joined from their capitals. The meeting itself was an instance of digital diplomacy. The tweets that followed on Twitter as part of the cyberspace were also digital diplomacy.

But cyber diplomacy, as a tool of grand strategy of a nation state to affect the cyber domain is very different. Sticking with our example of a NATO senior decision-makers meeting, let us examine how NATO member states conduct cyber diplomacy proper. NATO's mutual defence clause, Article 5 of the Washington Treaty, states the following:

> "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.
> Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security."[15]

[14] André Barrinha – Thomas Renard: Cyber-diplomacy: The Making of an International Society in the Digital Age. *Journal of Global Affairs,* 3, nos. 4–5 (2017). 353–364.

[15] North Atlantic Treaty Organization: *The North Atlantic Treaty. Washington D.C. – 4 April 1949. Article 5.* 10 April 2019.

But would an instance of a Russian hacker that disables the national banking computer system of a NATO member state fit this criteria? Is that an armed attack? Legal scholars were conflicted by the issue. So the Alliance took action through cyber diplomacy: it announced that a cyberattack could trigger Article 5 of our founding treaty at a NATO Summit in Wales in 2014, and later other Cyber Defence Pledges were taken as well. This type of general cyber diplomacy action constitutes a broader category, and of course incorporates direct instances of practical cyber diplomacy, i.e. the concrete steps of diplomacy that happen in the cyber, computer and informational technological world; it is a broader type of policy – a set of diplomatic actions that a state undertakes that affect the cyber domain.

Nevertheless, NATO took a more proactive stance to combat this ambiguity. In 2016, Allied Ministers issued a Cyber Defence Pledge, which, while not naming Article 5, took note of the following:

(1) In recognition of the new realities of security threats to NATO, we, the Allied Heads of State and Government, pledge to ensure the Alliance keeps pace with the fast evolving cyber threat landscape and that our nations will be capable of defending themselves in cyberspace as in the air, on land and at sea.

(2) We reaffirm our national responsibility, in line with Article 3 of the Washington Treaty, to enhance the cyber defences of national infrastructures and networks, and our commitment to the indivisibility of Allied security and collective defence, in accordance with the Enhanced NATO Policy on Cyber Defence adopted in Wales. We will ensure that strong and resilient cyber defences enable the Alliance to fulfil its core tasks. Our interconnectedness means that we are only as strong as our weakest link. We will work together to better protect our networks and thereby contribute to the success of Allied operations.[16]

In addition, the Alliance also decided to act on seven action items, all of which would deserve to be analysed on their own, but I list them here as potential actions of multilateral cyber diplomacy.

(1) Develop the fullest range of capabilities to defend our national infrastructures and networks. This includes: addressing cyber defence at the highest strategic level within our defence related organisations, further integrating cyber defence into operations and extending coverage to deployable networks; (2) Allocate adequate resources nationally to strengthen our cyber defence capabilities; (3) Reinforce the interaction amongst our respective national cyber defence stakeholders to deepen co-operation and the exchange of best practices; (4) Improve

[16] North Atlantic Treaty Organization: *Cyber Defence Pledge.* 08 July 2016.

our understanding of cyber threats, including the sharing of information and assessments; (5) Enhance skills and awareness, among all defence stakeholders at national level, of fundamental cyber hygiene through to the most sophisticated and robust cyber defences; (6) Foster cyber education, training and exercising of our forces, and enhance our educational institutions, to build trust and knowledge across the Alliance; (7) Expedite implementation of agreed cyber defence commitments including for those national systems upon which NATO depends.[17]

These Cyber Defence Pledge action items, which NATO follows up and continues to place emphasis on, are not the only actions this multilateral alliance has taken in the cyber realm. Further, NATO member states adopted the Tallinn Manual, showcasing their approach to cyber diplomacy – a rules based approach to the cyber realm. The Tallinn Manual has two editions, one from 2013 and an updated one from 2017. The newer, 2017 edition covers a

> "full spectrum of international law applicable to cyber operations ranging from peacetime legal regimes to the law of armed conflict, covering a wide array of international law principles and regimes that regulate events in cyberspace. Some pertain to general international law, such as the principle of sovereignty and the various bases for the exercise of jurisdiction. The law of state responsibility, which includes the legal standards for attribution, is examined at length. Additionally, numerous specialised regimes of international law, including human rights law, air and space law, the law of the sea, and diplomatic and consular law, are examined in the context of cyber operations."[18]

Nevertheless, it is important to note that while the Tallinn Manual and the NATO group of countries have their own alliance and policies advocating the liberalisation of cyberspace, countries in the Shanghai Cooperation Organisation advocate National Cyber Sovereignty, a fundamentally different approach.[19] The two approaches are at odds with each other and we will witness the greatest cyber diplomacy in the ongoing and future conflicts in the cyber realm.

After that introduction, the rest of the chapter examines the conceptually useful terms one needs to be aware of in the cyber realm. As with most literature on diplomacy as the conduct between states, cyber diplomacy is theorised about and analysed within the journal of international relations. As a subfield of political science, international relations focuses on the interactions between states and

[17] Ibid.
[18] CCDCOE: *The Tallin Manual.* 2017.
[19] Cyber Peace Alliance (2019): op. cit.

has three major paradigms: realism, liberalism and constructivism. These three, focusing on the role of power, reciprocity and norms in general, link how the cyber realm and cyber diplomacy within it, break up the literature on the topic fairly well.

Cyber Diplomacy in Theory

As is evident by now, cyber is in a realm of its own. Thus, there is a theoretical imperative to classify it in some manner, or to liken the topic to something else. It would be easy to classify a new topic as sui generis, i.e. that it has not ever been seen before and is not comparable to anything else. The most widespread use of this term in international relations theory applies to the European Union, which is, as much as there can be consensus in academic literature, sui generis. As the European Union can be understood to be an intergovernmental organisation, a supranational endeavour, a spirit or Zeitgest, a regional security organisation, and a myriad of other things, all valid from their own perspective, the argument holds. But cyber diplomacy is not sui generis and in fact is mostly understood to be a concept that has precedents in international, intersocietal and intra-societal relations.

Etymologies, Conceptualisations and Definitions

Before we explore the limits of cyber diplomacy, the question is what exactly does the term cyber mean and where would cyber diplomacy operate. As a quick reminder, in general analysts use the prefix 'cyber' to refer to a variety of digital, wireless and computer-related activities. But differences persist, and the approach one takes to the definition varies. The mandate of organisations that deal with some part of the cyber realm usually dictates the approach.

The U.S. Department of Defense, for example, defines

> "*cyberspace* as a global domain within the information environment consisting of the interdependent networks of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers and *Cyberspace operations* as the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace."[20]

[20] Kamaal T. Jabbour – Paul E. Ratazzi: Does the United States Need a New Model for Cyber Deterrence? In Adam B. Lowther (ed.): *Deterrence.* New York, Palgrave Macmillan, 2012. 33.

Of course, for them, the focus is on the military angle. Specifically, the U.S. military refers to cyber as a domain or sector of action (like land, sea, air and space), but it is also sometimes used to refer to a range of instruments or tools that can be employed along with others across a number of sectors.[21]

But what do foreign ministries do? Let us examine what the U.S. foreign ministry, the largest and most widely credited such organisation, the Department of State, writes on this topic.

> "The State Department is leading the U.S. Government's efforts to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation."[22]

Quite notably different from what the military does, but both are even more different from the realm of theory.

Cyber diplomacy in theory and in academic literature where the main locus of theoretical debates reside is a relatively recent entry, given the relatively recent introduction of the term in 2002 with a manuscript entitled *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century.* As such, the concept of cyber diplomacy is still conceptually contested. In fact, the manuscript in question meant only cyber diplomacy in practice, solely digital or e-diplomacy when it referred to the term. Since then, the peer-reviewed academic literature on the topic specifically of cyber diplomacy is relatively recent and somewhat under-published. Perhaps the most prominent example of this is a study entitled "Cyber-diplomacy: The Making of an International Society in the Digital Age", published in the Journal of Global Affairs, by Barrinha and Renard. The authors argue that cyber diplomacy, "which in spite of its rising importance [cyber diplomacy] has remained a peripheral issue in the International Relations (IR) literature".[23]

The authors argue that while cyber incidents, which this chapter details as well, has gained much more prominence in the media then cyber diplomacy.

As our analysis centres squarely on the level of states as actors, it is worth noting what other levels of analysis will certainly arise later. The upper echelon of

[21] Joseph S. Nye, Jr.: *The Future of Power.* New York, PublicAffairs, 2011b.
[22] U.S. Department of State: *Office of the Coordinator for Cyber Issues.* 2020.
[23] Barrinha–Renard (2017): op. cit. 354.

analysis, the "cyber international system", while feasibly a possibility to explore, is not quite at the level of academic theoretical analysis yet. This is no surprise; the study of foreign policy first amounted to exploring how states, as the most powerful actors in international relations, behaved. Only relatively recently, with the rise of structural or systemic explanations of patterns of interstate behaviour, did the systemic level of analysis prove useful. Thus while the analysis of the conduct of state behaviour dates back quite a while, only with Kenneth Waltz's *Theory of International Politics* of the 1960s did truly systemic levels of analysis begin. It is thus perfectly plausible that system levels of analysis for the cyber realm will arise in the future. This would focus on establishing certain components of the cyberspace that define the manner in which behaviour, including cyber diplomacy, could be conducted. Until then, I focus on the state-level with an eye for the international organisations that do work here as well, but some work on non-governmental organisations and actors that have a meaningful role to play in the cyber realm also.

To begin the state-level analysis, a search for a clear definition of cyber diplomacy provides a strong starting point. Given the relative dearth of academic literature, definitions are not too abundant. Most of these start with defining diplomacy and then link it to the cyber realm. We note that the definitions of diplomacy vary with whether power, reciprocity, or norms are the key drivers behind international relations for the authors. Thus diplomacy can for once be understood as the attempt to adjust conflicting interests by negotiation and compromise. For others, diplomacy is a central institution in the definition and maintenance of international society. As for the English School and for Hedley Bull, diplomacy is a custodian of the idea of international society, with a stake in preserving and strengthening it. For Bull, diplomatic practice has five main functions: to facilitate communication in world politics, to negotiate agreements, to gather intelligence and information from other countries, to avoid or minimise friction in international relations and, finally, to symbolise the existence of a society of states. Cyber diplomacy then is the conduct of such practices in the cyber realm. For Barrinha and Renard, "cyber-diplomacy can be defined as diplomacy in the cyber domain or, in other words, the use of diplomatic resources and the performance of diplomatic functions to secure national interests with regard to the cyberspace".[24]

Regardless of which definition one accepts, follow-on questions are intent on delimiting cyber diplomacy. If we accept the most general definition of cyber

[24] Ibid.

diplomacy, as the use of diplomatic resources to secure national interests with regard to the cyberspace, then what is it not? Conceptualisations must be made by clearly delimiting the term. Cyber diplomacy is then by definition, not cyber war, not cyber defence, not cybersecurity, and not cyber deterrence, cyber compellance, or cyber coercion. These terms would apply to the use of other types or national resources in some other way.

To continue the conceptualization process, the division between cyber diplomacy and cyber war or cyber warfare must be made. In sharp contrast to the academic theoretical analysis of cyber diplomacy, cyber war has been relatively well studied. The first question of course is whether cyber war can be understood to be warfare in the general sense. Stone's seminal piece from 2013 published in the notable *Journal of Strategic Studies,* entitled "Cyber War *Will* Take Place" clearly answers in the positive.[25] He determines that cyber warfare meets the criteria of the concepts of force, violence and lethality, and as such, should be able to be considered war. Of course others disagree somewhat, focusing on the fact that there is no agreed consent upon the definition of cyber war and cyber warfare, noting in particular that even the two are not quite readily distinguishable.[26] Joseph S. Nye, an authority on the topic, makes a similar point: "A more useful definition of cyber war is, hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence."[27] But cyber war is not by necessity simply an amalgamation of a number of cyberattacks (the term cyberattack covers a wide variety of actions ranging from simple probes, to defacing websites, to denial of service, to espionage and destruction). It is noticeably different from conventional wars. One such major difference is that "the barriers to entry in the cyber domain are so low that non-state actors and small states can play significant roles at low cost".[28] In conclusion, and underlining why we have to make sure we differentiate between the terms exactly, in the current literature the term "cyber war is used very loosely for a wide range of behaviours. In this, it reflects dictionary definitions of war that range from armed conflict to any hostile contention".[29]

[25] John Stone: Cyber War *Will* Take Place! *Journal of Strategic Studies,* 36, no. 1 (2013). 101–108.
[26] Michael Robinson et al.: Cyber Warfare: Issues and Challenges. *Computers and Security,* 49 (2015). 70–94.
[27] Nye (2011a): op. cit. 21.
[28] Ibid. 20.
[29] Ibid.

The Purpose of Cyber Diplomacy

What function one purports cyber diplomacy to serve depends significantly on one's look on how the international system functions. As such, the most useful manner in which to conceptually categorise the literature is to follow the three major paradigms of international relations. As a reiteration, this categorisation is interested in literature on cyber diplomacy proper, and not on what is conceptually covered under the term digital or e-diplomacy.

The literature on cyber diplomacy falls under three broad categories. The first is interested in grappling with the linkages of cyber diplomacy to power; the second, to reciprocity and interdependence, many times through the use of law and legal treaties; and the third, linkages to norms and patterns of behaviour. It is thus not surprising that the three major schools of thought, realism, liberalism and constructivism is what is used here to create these categories.

Broadly speaking, cyber diplomacy also takes place in what scholars of international relations theory would label as the condition of anarchy. There is no supra-national 'cyber authority' in the world, and the realm of cyber is, and often here only partially and superficially, regulated by governments. One, thus, could assume that cyber diplomacy follows similar rules to what diplomacy between states follows. But unlike traditional diplomacy and its counterpart, war, three major differences of state behaviour are clearly visible, all of which are polar opposites between traditional and cyber diplomacy.

The first is that the assets, parts, individuals and components of cyber diplomacy lack a clear spatial designation. They are interspersed throughout our globe and are interconnected in ways that make clearly separable modes of power distinction unrealistic. For regular diplomacy, an Ambassador Extraordinary and Plenipotentiary is the clear, singular fount of sender state jurisdiction in the host state. The Ambassador is a single person, and only holds this special capacity while in host country, as dictated by a bilateral agreement covered in the international treaty known as the Vienna Convention on Diplomatic Relations of 1961. For the cyber world, by definition, the bits and bytes that actually contain data that is used as the medium for cyber diplomacy is spread out. Efforts and policy, in the same vein, that target cyber issues, cannot be spatially bound. This makes the matter much more complex and interdependent, where lines of demarcation are not readily apparent.

A second issue is the question of intermediaries or the degrees of separation of action. In traditional diplomacy, once the Ambassador is absent, his deputy

assumes this role, usually under the title of charge d'affaires. If for some reason an Ambassador is not present for an extended period of time, the charge d'affaires becomes ad interim, a.i., and assumes the role of the Ambassador. In cyber diplomacy, there are numerous intermediaries that may come between the policy and the effect of the policy or the start state and the end result. A Russian Government Directive may result in the government tasking an intelligence directorate, which is still part of the state apparatus. The intelligence director then asks a private hacker to fulfil a request, who then outsources it to a hacker in Belgium but who is a South African national. The intermediaries are numerous and vary between public and private.

Third and finally, in much the same vein how cyber demarcation is hardly possible, as Virtual Private Networks for example mask our I.P. addresses, the issue of attribution surfaces as well. Reverting back to our traditional diplomatic example, attribution is quite simply taken for granted: in fact, only quite readily attributable diplomats and diplomatic instances are allowed in the host state. Attribution is a key component in traditional diplomacy. In cyber diplomacy, and in the cyber realm writ large, attribution or more specifically the lack of credible attribution, is a fundamental issue. Cyber incidents have clear end-points. Distributed Denial of Service Attacks (DDoS) clearly affect host computers or websites which are shut down. But where the attack originates is a much more complex issue and at many times impossible to determine with any degree of certainty. Deputy Secretary of Defense William Lynn wrote in 2010: "Whereas a missile comes with a return address, a computer virus generally does not. The forensic work necessary to identify an attacker may take months, if identification is possible at all."[30] Or for example in the Stuxnet attack of 2010, the question of verifiable attribution is foundationally uncertain even today, although there is a clear consensus that it was a joint operation of the United States and Israeli governments.

Thus cyber diplomacy operates in a space that is clearly different, in fact quite the opposite of the realm of traditional diplomacy. It is geographically unbound, operates with potentially significant chains of intermediaries where functions and roles differ significantly, and is in a plethora of cases virtually without credible attribution. And while almost all scholars agree on these differences, the role of cyber diplomacy is best examined through the lenses of international relations theories.

[30] William J. Lynn III: Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs,* 89, no. 5 (2010). 99.

Cyber Diplomacy and Power

One chain of thought that connects literature on cyber diplomacy is the realist approach. Here authors are primarily interested in how cyber diplomacy can act as a complement to efforts of war and violence; that is, diplomacy in itself is meaningless, only in juxtaposition (or at times subjugation) to military efforts can it be understood. Cyber diplomacy here is often simply considered a function of an exertion of power in the national interest by states.

Many authors focus on the role of cyber diplomacy as a function of cybersecurity and examine whether cyber diplomacy can affect cyberattacks. As Nye writes: "There are three main vectors of cyberattack: via networks, via supply chains, and by human insiders who may be malicious or just careless. Disconnecting from the network is costly, and the "air gaps" it creates do not guarantee security."[31] Others are intent on differentiating between the levels of cyber defence.[32] O'Connell for example points out that the U.S. has clearly pursued a realist approach, by first setting up and devoting sizable funds to the U.S. Department of Defense and the armed services.[33] This of course raises the question of the legality of action in the cyber realm, and here O'Connell exposes the deep divide between approaches. Here the question of attributing intent is one of the key issues, called AIOS by experts. AIOS stands for *attacker intent, objectives and strategies,* and academics have even attempted to present a "general incentive-based method to model AIOS and a game-theoretic approach to inferring AIOS".[34] Further, if cyber diplomacy is merely an extension of cyber warfare, then the question of deterrence comes to mind. Here cyber diplomacy is the sum of efforts that would make deterrence credible. Some point out that "the attribution problem appears to make retaliatory punishment, contrasted with defensive denial, particularly ineffective".[35]

[31] Joseph S. Nye, Jr.: Deterrence and Dissuasion in Cyberspace. *International Security,* 41, no. 3 (2016). 44–71.

[32] Dorothy E. Denning: Framework and Principles for Active Cyber Defense. *Computers and Security,* 40 (2014). 108–113.

[33] Mary Ellen O'Connell: Cybersecurity Without Cyber War. *Journal of Conflict and Security Law,* 17, no. 2 (2012). 187–209.

[34] Peng Liu – Wanyu Zang: Incentive-Based Modeling and Inference of Attacker Intent Objectives, and Strategies. *ACM Transactions on Information and System Security (TISSEC),* 8, no. 1 (2005). 80.

[35] Jon R. Lindsay: Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack. *Journal of Cybersecurity,* 1, no. 1 (2015). 53.

Further, notable scholars argue that

> "many of the properties of cybersecurity assumed to be determined by technology, such as the advantage of offense over defense, the difficulty of attribution, and the inefficacy of deterrence, are in fact consequences of political factors like the value of the target and the scale-dependent costs of exploitation and retaliation".[36]

This, in line with traditional realist arguments, does not agree that the cyber realm is sui generis by nature. Geers for example made a compelling comparison between cyber diplomatic efforts that complement cyber deterrence and nuclear deterrence, by analysing "two deterrence strategies available to nation-states (denial and punishment) and their three basic requirements (capability, communication, and credibility) in the light of cyber warfare".[37] As such, deterrence is critically important. But some question the point of transference of nuclear deterrence to the cyber world. Richard Clark and Robert Knake for example argue that "of all the nuclear strategy concepts, deterrence theory is probably the least transferable to cyber war".[38] And noted Columbia Professor Richard Betts has argued that deterrence does not work well in cyberspace because of the problem of attribution.[39] Others, quite naturally, completely disagree and instead search for a new paradigm in cyber deterrence, criticising "the current discourse in the field, including some 'common knowledge' (mis)understandings of cyberspace and the ways it affects the possibility of deterrence".[40]

The question of how far cyber diplomacy extends, of course, does not stop with assuming that power is solely interested in traditional methods of warfare. The debate about the role of national interest and diplomatic efforts versus military efforts is also picked up in the topic of cyber terrorism. Some, like Hua and Bapna, examine the interlinkages of cyber terrorism with the possible economic

[36] Ibid.

[37] Kenneth Geers: The Challenge of Cyber Attack Deterrence. *Computer Law and Security Review,* 26, no. 3 (2010). 302.

[38] Richard A. Clark – Robert K. Knake: *Cyber War: The Next Threat to National Security and What to Do About It.* New York, Harper Collins, 2010. 189.

[39] Richard K. Betts: The Soft Underbelly of American Primacy: Tactical Advantages of Terror. *Political Science Quarterly,* 117, no. 1 (2002). 19–36.

[40] Uri Tor: 'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence. *Journal of Strategic Studies,* 40, nos. 1–2 (2015). 92.

impact.[41] Others focus on determining whether the level of threat, that is usually taken for granted, truly can be assessed in a valid manner as such. For example Brunst writes: "Although it is known that terrorists already routinely use the Internet for purposes such as spreading propaganda or conducting internal communication, the threat that results from this use is heavily debated."[42] Finally, how useful can cyber coercion be? One of the most studied examples is the 2014 North Korean operation against Sony. While there are still multiple aspects that are not fully developed, the widely shared narrative argues that "through cost imposition and leadership destabilization, the North Korean operation, despite its lack of physical destructiveness, caused Sony to make a series of costly decisions to avoid future harm."[43]

This is a major challenge to the conventional wisdom that cyber operations cannot conduct successful coercion. In fact, as this demonstrates, it is perfectly feasible, as costs mount and the expected utility of capitulation surpasses the costs of defiance. Guarding against coercion of course requires resilience. But when it comes to cyber resilience, "there is a dawning realisation that the best technical solutions offer only partial assurance. Paradoxically, in an era when the Internet seems ubiquitous, a mixture of analogue and manual systems – often called systems diversity – offers a solution."[44]

In short, realist approaches to cyber diplomacy focus on traditional themes that are also present in international relations literature from a realist perspective elsewhere. The role of power is paramount, and the most analysed form for the use of power is through military means. Cyber diplomacy is defined and examined as a complement to the use of force, specifically as an addition to deterrence, compellance, coercion and even war. Unsurprisingly, linkages to the economy are examined from an International Political Economy perspective. The securitisation of cyber diplomacy is bound to follow on the pages of relevant journals as well, as it has clearly begun with the literature on cyber terrorism.

[41] Jian Hua – Sanjay Bapna: The Economic Impact of Cyber Terrorism. *The Journal of Strategic Information Systems,* 22, no. 2 (2013). 175–186.

[42] Phillip W. Brunst: Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet. In Marianne Wade – Almir Maljevic (eds.): *A War on Terror?* New York, Springer, 2010. 51.

[43] Travis Sharp: Theorizing Cyber Coercion: The 2014 North Korean Operation against Sony. *Journal of Strategic Studies,* 40, no. 7 (2017). 898.

[44] Lewis Herrington – Richard Aldrich: The Future of Cyber-Resilience in an Age of Global Complexity. *Politics,* 33, no. 4 (2013). 299.

The already established use of force linkages established in the nuclear proliferation literature surface here as well, with articles examining the possibility of deterring cyber terrorists.

But as with all research programs, such as realist agendas in international relations theory, a paradigm shift is sometimes called for. Sharma for example argues that

> "the last couple of decades have seen a colossal change in terms of the influence that computers can have on the battlefield. [The article] tries to shatter myths woven around cyber warfare so as to illuminate the strategic aspects of this relatively misinterpreted notion, thus identifying a paradigm shift, making cyber war the primary means of achieving grand strategic objectives in the contemporary world order."[45]

But when a paradigm shift may actually happen is a matter of debate and uncertainty, and in academic literature, may take time.

Cyber Diplomacy and Reciprocity

Another broad bucket of international relations literature takes a different approach to cyber diplomacy and highlights other priorities. Instead of focusing on cyber diplomacy as a complement to military and use of force, the large house of liberalism focuses on interdependence, international organisations, reciprocity between state actors and legal treaties as central tenets. This set of literature highlights the central role of cyber diplomacy in regulating cyberspace and increasing cybersecurity. Here the efforts of authors begin with the core ideas of liberalism or liberal institutionalism: economic interdependence, the role of international organisations and the democratic peace theory.

Beginning with economic interdependence, the authors here focus on how cyber diplomacy could be used to mitigate issues that may affect cybersecurity. Hausken for example highlights the role of income and substitution effects in cyberspace.[46] In his journal article, Hausken uses the Sarbanes-Oxley Act to demonstrate that when such an act

[45] Amit Sharma: Cyber Wars: A Paradigm Shift from Means to Ends. *Strategic Analysis,* 34, no. 1 (2010). 62.

[46] Kjell Hausken: Income, Interdependence, and Substitution Effects Affecting Incentives for Security Investment. *Journal of Accounting and Public Policy,* 25, no. 6 (2006). 629–665.

> "strengthens internal controls, and the government encourages information sharing, accounting gains significance through secure representation, storage, and transfer of information, and by laying the foundation for assessing costs and benefits, resulting in individual optimization implying free riding."[47]

Other authors who can be argued to fall under the broad liberal agenda focus on the role of information sharing as a form of interdependence, by highlighting that as "the Internet threat landscape is fundamentally changing, a major shift away from hobby hacking toward well-organized cyber crime can be observed [and] new paradigms are required for detecting contemporary attacks and mitigating their effects".[48] Other forms of interdependence are examined from a liberal angle as well, even those of the military, but these are somewhat more nuanced. On article argues that "the globalization and increasing complexity of modern cyber security operations have made it virtually impossible for any organization to properly manage cyber threats and cyber incidents without leveraging various collaboration instruments with different partners and allies".[49] This of course postulates that cyber diplomacy is most efficiently served through interdependence, even when it comes to issues of cybersecurity.

In addition to interdependence, many discussions centre on Internet freedom as well, and the interlinkages with political economy abound as well. Shawn Powers and Michael Jablonski "conceptualize this real cyber war as the utilization of digital networks for geopolitical purposes, including covert attacks against another state's electronic systems, but also, and more importantly, the variety of ways the Internet is used to further a state's economic and military agendas".[50] The State Department is singled out as an actor that is looking to connect actors in the cyber realm. Others highlight the role of the State Department and argue that cyber diplomacy is only a smaller portion of a larger whole, namely public diplomacy. One prime example is Cull's article, which lists seven lessons of public diplomacy, namely: (1) public diplomacy begins with listening; (2) public diplomacy must be connected to policy; (3) public diplomacy is not a

[47] Kjell Hausken: Information Sharing among Firms and Cyber Attacks. *Journal of Accounting and Public Policy,* 26, no. 6 (2007). 639.

[48] Ibid.

[49] Jorge L. Hernandez-Ardieta – Juan E. Tapiador – Guillermo Suarez-Tangil: Information Sharing Models for Cooperative Cyber Defence. In *2013 5th International Conference on Cyber Conflict (CYCON 2013).* IEEE. 1.

[50] Shawn M. Powers – Michael Jablonski: *The Real Cyber War. The Political Economy of Internet Freedom.* Champaign, IL, University of Illinois Press, 2015. 2.

performance for domestic consumption; (4) effective public diplomacy requires credibility, but this has implications for the bureaucratic structure around the activity; (5) sometimes the most credible voice in public diplomacy is not one's own; (6) public diplomacy is not "always about you"; and (7) public diplomacy is everyone's business, and demonstrates how these also apply to cyber diplomacy.[51]

One of the most critical components of liberal tenets is reciprocity, mainly through equal treatments and legal guarantees. Two major venues of analysis are examined in this approach. The first usually links cyber diplomacy to international legal treaties, in no small part to International Humanitarian Law. The second focuses on the legal use of force and where cyberattacks warrant a cyber diplomatic response and where they would fall under the purview of the military.

International humanitarian law is one issue that is under scrutiny in the cyber diplomatic realm. One key article attempts to examine this specific issue. It asks the following question: when is cyber war really war in the sense of 'armed conflict'? Powers and Jablonski go on to look at some of the most important rules of

> "IHL governing the conduct of hostilities and the interpretation in the cyber realm of those rules, namely the principles of distinction, proportionality, and precaution. With respect to all of these rules, the cyber realm poses a number of questions that are still open. In particular, the interconnectedness of cyber space poses a challenge to the most fundamental premise of the rules on the conduct of hostilities, namely that civilian and military objects can and must be distinguished at all times."[52]

Of course, in liberal international relations tenets the question of the use of force is also examined, but through a legal lens. Here cyber diplomacy is also approached through this lens. Buchan for example argues that the "legality of cyberattacks is generally approached from the use of force prohibition contained in Article 2(4) UN Charter".[53] He goes on to ask whether an unlawful use of force in the cyber realm can be squared with the fact that an intervention must produce physical damage. Simply stated, a cyberattack can cause physical damage and therefore violate Article 2(4), but what if it does not? Questions on this are not yet resolved in theory nor in policy.

[51] Nicholas J. Cull: Public Diplomacy: Seven Lessons for Its Future from Its Past. *Place Branding and Public Diplomacy,* 6, no. 1 (2010). 11.

[52] Cordula Droege: Get Off my Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians. *International Review of the Red Cross,* 94, no. 886 (2012). 533–578.

[53] Russell Buchan: Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? *Journal of Conflict and Security Law,* 17, no. 2 (2012). 212.

Finally, scholars question whether the existing legal framework in the cyber realm is sufficient for cyber diplomacy to function properly. Turns writes: "The domain of cyber warfare being relatively new, it is not yet matched by any comparatively novel international legal paradigm; the cyber conflicts of the present and (probably) the future therefore fall to be regulated under the existing lex lata."[54] If cyber warfare lacks regulation, then the first priority of cyber diplomacy should be to establish such rules.

In conclusion, liberal approaches to cyber diplomacy focus on the theoretical linkage between already established key concepts, such as economic interdependence, rule of law and international organisations. They are adapted to be functions that cyber diplomacy can fulfil. But the linkages are not always readily apparent in theory at least. One clear argument, in line with how nuclear non-proliferation talks have gone, is the reciprocal disarmament vein. Here there are certain issues, as the largest player in the world who could champion this is currently its most capable military actor as well. As Gjelten argues,

> "the US disadvantage would be compounded by the fact that, by most analyses, no other military has such an advanced offensive capability for cyber war. Under a comprehensive cyber arms limitation agreement, the US would presumably have to accept deep constraints on its use of cyber weapons and techniques."[55]

But when it comes to the economic realm,

> "from a security perspective, there is a misalignment of economic incentives in the cyber domain. Firms have an incentive to provide for their own security up to a point, but competitive pricing of products limits that point. Moreover, firms have a financial incentive not to disclose intrusions that could undercut public confidence in their products and stock prices."[56]

This of course complicates issues here, but as with many economic theories, norms govern our behaviour sometimes unbeknownst to us.

[54] David Turns: Cyber Warfare and the Notion of Direct Participation in Hostilities. *Journal of Conflict and Security Law,* 17, no. 2 (2012). 279.

[55] Tom Gjelten: Shadow Wars: Debating Cyber 'Disarmament'. *World Affairs,* 173, no. 33 (2010). 33.

[56] Nye (2011a): op. cit. 28.

Cyber Diplomacy and Norms

A final large group of approaches to cyber diplomacy can be categorised under the broad paradigm of international relations, constructivism. When it comes to examining cyber diplomacy, these theoretical works highlight the importance of social constructions, identity and norms. Here the works focus mainly not on the cyberattacks or incidents themselves, as those are given, but instead attempt to figure out why the attacks or incidents occur and what explains their drivers and outcomes. It is not that the "cyberattacks" are thought to be social constructs, but rather their effect and causes are argued to be governed by principles that are constructed in nature.

For example, the role of norms can be used to assess whether there will be an increase in frequency of cyberattacks. One approach that Valeriano and Maness take is highlighting that "restraint is the norm in cyberspace and suggests that there is evidence this norm can influence how the tactic is used in the future".[57] They argue that norms are the most prominent drivers of state behaviour in the constructivist vein, and their theory of cyber conflict is predicated on empirical patterns. An alternate view is that norms are not quite as widespread across the cyber realm as Valeriano and Maness argue, but in fact, the norms vary significantly across states and within their pattern of behaviour. Kshetri argues that symbolic significance and criticalness, degree of digitisation of values and weakness in defence mechanisms are the key factors, and not norms that determine whether restraint or more aggressive cyberattacks are taken.[58]

Of course, the follow on question is equally important. Why bother with cyber diplomacy? Is cyber war even likely? Junio argues in "How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate" that, in line with the offense–defence theory, cyber weapons will most likely be used offensively, and makes the argument that they will be done because of the principal agent problem.[59] Another argument in the same journal, by Liff, set forth in an article that examines proliferation of cyberwarfare capabilities and its

[57] Brandon Valeriano – Ryan C. Maness: *Cyber War versus Cyber Realities. Cyber Conflict in the International System.* New York, Oxford University Press, 2015. 32.

[58] Nir Khsetri: Pattern of Global Cyber War and Crime: A Conceptual Framework. *Journal of International Management,* 11, no. 4 (2005). 541–562.

[59] Timothy J. Junio: How Probable Is Cyber War? Bringing IR Theory Back In to The Cyber Conflict. *Journal of Strategic Studies,* 36, no. 1 (2013). 125–133.

implications for the character and frequency of war. Here the author is of the opinion that "strategic logic, perceptions, and bargaining dynamics finds that the size of the effect of the proliferation of cyberwarfare capabilities on the frequency of war will probably be relatively small".[60] This is of course in line with what we have seen in practice as well with Stuxnet. Probably, the most widely cited study of this is Farwell and Rohozinski's work in *Survival,* where the authors demonstrate that there is a striking confluence between cybercrime, cyber threats, and state actions.[61]

The opposite has been argued as well, that cyberwar in fact will not take place, because "all politically motivated cyberattacks are merely sophisticated versions of three activities that are as old as warfare itself: sabotage, espionage, and subversion".[62] Here Rid, writing for the Journal of Strategic Studies, argues that "cyber war has never happened in the past, that cyber war does not take place in the present, and that it is unlikely that cyber war will occur in the future".[63] The argument of course, and the division over the debate is about definitions of the purpose, scope and motivation of cyberattacks, and whether they meet the criteria of cyberwar. Yet it seems that this debate has been roughly concluded. While the side arguing for cyberattacks to not meet the threshold of cyberwar, the argument that there are easy connections between cyberattacks and kinetic responses and outcomes clearly link cyber events to acts of war, and states, for example NATO's Article 5 and U.S. policy statements, clearly are in line with this analytical approach.

The argument most closely mirroring this is McGraw's "Cyber War is Inevitable (Unless We Build Security In)".[64] This piece's argument, i.e. information systems controlling our critical infrastructure are vulnerable to cyberattacks, and as such, cyberwar is therefore inevitable unless we improve our cyber defences, is the approach that most governments have taken and will be explored deeply in the Cyber Diplomacy in Policy Portion. Of course, others point out that there is no readily accepted level that reaches this threshold.

[60] Adam P. Liff: Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies,* 35, no. 3 (2012). 401.

[61] James P. Farwell – Rafal Rohozinski: Stuxnet and the Future of Cyber War. *Survival,* 53, no. 1 (2011). 23–40.

[62] Thomas Rid: Cyber War Will Not Take Place. *Journal of Strategic Studies,* 35, no. 1 (2012). 5.

[63] Ibid.

[64] Gary McGraw: Cyber War Is Inevitable (Unless We Build Security In). *Journal of Strategic Studies,* 36, no. 1 (2013). 109–119.

> "Computer Network Attacks (CNAs) do not automatically come within the framework of the definition of 'attack' in conformity with the law of armed conflict (LOAC). Consequently, some so-called CNAs (especially, those used only as means of intelligence gathering) do not qualify as 'attacks'."[65]

The debate will continue here, but policy may lead and theory may only follow.

What we have witnessed in this section is a similar nuclear non-proliferation debate of the Cold War. In the middle of the Cold War, debates were held, most notably between Kenneth Waltz and Scott Sagan, about whether the spread of nuclear weapons will increase or decrease stability in the international system. Waltz argued that the more states with nuclear weapons, the more stability in the system, as nuclear weapons disincentive warfare by raising its cost. Sagan argued the opposite, mainly focusing on misappropriation, mistakes, and miscalculations.[66] Interestingly, a policy consensus arose over Sagan's approach, endorsed by even "realist" political leaders who would have otherwise agreed with Waltz's approach of state pattern of behaviour. Once the consensus developed, the nuclear-non-proliferation regime began in earnest. The signing of the Treaty on Nuclear Non-Proliferation began the era, but the Intermediate and Medium-Range Nuclear Forces Treaty, the Strategic Arms Limitations Talks I and II, the Strategic Arms Reduction Talks I, II and III, and the Fissile Material Cut-off Treaty, the Comprehensive Test Ban Treaty all followed. The state groupings such as the Wassenaar Group, the Zangar Commission and other formats followed. If the cyber diplomatic realm follows suit, then once the consensus on how to conceptualise cyber war emerges, cyber diplomatic efforts will follow. The following section presents some of these efforts and anticipates the potential future for some others.

Unsurprisingly there is a prevalent counter-argument. Lawson

> "argues that current contradictory tendencies are unproductive and even potentially dangerous. [His article] argues that the war metaphor and nuclear deterrence analogy are neither natural nor inevitable and that abandoning them would open up new possibilities for thinking more productively about the full spectrum of cyber security challenges, including the as-yet unrealized possibility of cyber war."[67]

[65] Yoram Dinstein: The Principle of Distinction and Cyber War in International Conflicts. *Journal of Conflict and Security Law,* 17, no. 2 (2012). 261.

[66] Scott Sagan et al.: A Nuclear Iran: Promoting Stability or Courting Disaster? *Journal of International Affairs,* 60, no. 2 (2007). 135–150.

[67] Sean Lawson: Putting the "War" in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States. *First Monday,* 17, no. 7 (2012).

As with the nuclear non-proliferation debate, which leads and which follows is yet to be determined.

As within the pages of international relations journals, the most ventures away from states and organisations as actors are to be found in the constructivist groups of works. De Bruijn and Janssen highlight the need to bring individuals into the framework of assessment. They showcase that while everybody has heard of cybersecurity, still, the urgency and behaviour of individuals' actions do not reflect a high level of awareness.[68] The authors "discuss the challenges in framing policy on cybersecurity and offer strategies for better communicating cybersecurity. Communicating cybersecurity is confronted with paradoxes, which has resulted in society not taking appropriate measures to deal with the threats" – which, as they attempt to highlight, can be best done by putting the issues in perspective.[69]

Finally, there are of course works that attempt to demonstrate that even the virtual space designated for cyberspace is somewhat a construct. Barnard-Wills and Ashenden's article "examines the problems of construction of virtual space and current efforts to secure this space political and technologically".[70] The authors present a model of cybersecurity discourse that is argued to be ungovernable, unknowable, a cause of vulnerability, inevitably threatening and a home to threatening actors. It is in this vein that cyber diplomacy has to operate, but there is a major challenge the authors present actors in the cyber diplomatic realm with: should they attempt to conduct cyber diplomacy in a cyber realm governed by this modus operandi or attempt to alter the fundamental underlying discourse? The pattern of behaviour, or even the ethics of which type of cyber diplomacy has been conducted, can also be at least tangentially explored by examining its counterpart, war. Lucas argues that cyber "technologies offer prospects for lessening the indiscriminate destructive power of war, and enhance prospects for the evolution from state-centred conventional war, to discriminate law enforcement undertaken by international coalitions of peacekeeping forces".[71]

[68] Hans de Bruijn – Marijn Janssen: Building Cybersecurity Awareness: The Need for Evidence-based Framing Strategies. *Government Information Quarterly,* 34, no. 1 (2017). 1–7.

[69] Ibid. 1.

[70] David Barnard-Wills – Debi Ashenden: Securing Virtual Space: Cyber War, Cyber Terror, and Risk. *Space and Culture,* 15, no. 2 (2012). 110.

[71] George R. Lucas, Jr.: Postmodern War. *Journal of Military Ethics,* 9, no. 4 (2010). 289.

As Nye writes

> "norms can be suggested and developed by a variety of policy entrepreneurs. For example, the new non-governmental Global Commission on Stability in Cyberspace, chaired by former Estonian Foreign Minister Marina Kaljurand, has issued a call to protect the public core of the Internet (defined to include routing, the domain name system, certificates of trust, and critical infrastructure)."[72]

Practitioners of cyber diplomacy should well keep all this in mind.

Cyber Diplomacy in Policy and Practice

The theoretical differentiation is, of course, only one aspect of the review of the literature of cyber diplomacy. Another key component is the review of literature that examines not theoretical issues, conceptualisations, definitional squabbles, or operationalised variables, but concrete state policies in concrete issues both at the state and at the intergovernmental level, namely the UN. The goal of this chapter is not to provide a detailed analysis of each, but rather to give a glimpse into the various national and international actors who are most involved in the world of cyber diplomacy.

Here the literature is much more varied and vast, but much more dispersed as well. Larger case studies may incorporate some angles of diplomacy, some of which may be cyber diplomacy, but that foray would be too large to present here. Instead, articles and reports are selected, which attempt to capture writings that grapple with some larger diplomatic or strategic issues and incorporate a significant cyber component, as well. The prime actor, of course, is still the United States as a hegemon, but the U.S. has already been examined here in various ways.

As with many newer topics in international relations, the question of the rise of China is also examined in a cyber diplomatic context. While this is not the most frequently studied question in cyber diplomacy, the Covid-19 crisis has exacerbated the issue significantly. On the one hand, a battle of narratives is happening, with a significant prize at the end, including in electronic media and as such e-diplomacy. Further, the Covid-19 pandemic will most likely accelerate

[72] Joseph S. Nye, Jr.: How Will New Cybersecurity Norms Develop? *Project Syndicate,* 08 March 2018.

the digital transformation, leading to an increase in digital diplomacy, too. The question of this chapter is fundamentally the broader issue of cyber diplomacy so only selected works are presented here.

One of the fundamental works on the topic attempts to reconcile the U.S.–China relationship in the cyber realm, with a focus on cybersecurity and as such, cyber diplomacy. Lindsay's work highlights the "exaggerated fears about the paralysis of digital infrastructure and the loss of competitive advantage contribute to a spiral of mistrust in U.S.–China relations".[73] But perhaps the most significant addition of Lindsay's work is the extension of the great power hegemonic struggle into the cyber realm. Lindsay argues that the "cyber version of the stability-instability paradox constrains the intensity of cyber interaction in the U.S.–China relationship – and in international relations more broadly – even as lesser irritants continue to proliferate".[74] In line with how the most recent assessments of this great power competition are examined, Lindsay's words may serve as a warning to the West when he writes: "China is resorting to a strategy of international institutional reform, but it benefits too much from multistakeholder governance to pose a credible alternative."[75] Of course, whether this is because of the fact that "although China also actively infiltrates foreign targets, its ability to absorb stolen data is questionable, especially at the most competitive end of the value chain, where the United States dominates", or a more deeply enshrined cooperation strategy by Beijing remains to be seen.

The second major actor where cases of cyber diplomacy can be studied is with Russia.[76] The rhetoric that surrounds cyber campaigns may be a key indicator in studying cyber diplomacy in the future. Here information shaping may play a key role. Deibert, Rohozinski, and Crete-Nishihata argue that "while the rhetoric of cyber war is often exaggerated, there have been recent cases of international conflict in which cyberspace has played a prominent role".[77] They study the case of Georgia and Russian actions in the conflict over the disputed territory of South Ossetia in August of 2008. The outcomes they highlight: the unavoidable

[73] Jon R. Lindsay: The Impact of China on Cybersecurity: Fiction and Friction. *International Security,* 39, no. 3 (2015). 8.

[74] Ibid. 46.

[75] Ibid. 13.

[76] Ibid. 44.

[77] Ronald J. Deibert – Rafal Rohozinski – Masashi Crete-Nishihata: Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War. *Security Dialogue,* 43, no. 1 (2012). 3.

internationalisation of cyber conflicts, and the tendency towards magnifying unanticipated outcomes in cyber conflicts, both increase the need for a more robust response in the cyber diplomatic realm, as well.

The most frequently associated follow on the topic after China and Russia has to do with terrorism, another widely studied topic in international relations. There usually are two approaches when it comes to cyber diplomacy: the first concerns cyber terrorism, and the relevant aspects such as cyber deterrence detailed earlier in this chapter, or the use of social media and digital diplomacy as a second large bucket. Awan's study, "Cyber-Extremism: Isis and the Power of Social Media" is a prime example.[78] Here the author argues that "these modern day tools are helping Isis spread their propaganda and ideology to thousands of online sympathizers across the world".[79] In fact, since the "Internet therefore is becoming the virtual playground for extremist views to be reinforced and act as an echo chamber", cyber diplomatic efforts must also combat these here.[80] Another study explores the connection between cyber warriors and the state, and argues that some such groups, for example the Syrian Electronic Army, is "closely connected to the Syrian government in order to serve two main goals: serving as a public relations tool for the Syrian government to draw the world's attention to the official Syrian version of events taking place in the country and countering the impact of Syrian oppositional groups".[81]

Finally, the United Nations as an actor in cyber diplomacy deserves significant analysis. It is both a platform for action by member states through the Security Council and an independent actor through the Secretariat on its own, headed by the Secretary-General. At the Security Council, the issues date back to 1998, when Russia first proposed a UN treaty to ban electronic and information weapons (this included its use for propaganda purposes). Russia, together with China and other members of the Shanghai Cooperation Organization, has continued to push for a broad UN-based treaty, but in contrast, the U.S. continues to view such a treaty as unverifiable.

When it comes to the Secretariat, the UN Secretary-General appointed a Group of Governmental Experts (UNGGE) which first met in 2004, and in July

[78] Imran Awan: Cyber-Extremism: Isis and the Power of Social Media. *Society,* 54, no. 2 (2017). 138–149.

[79] Ibid. 138.

[80] Ibid.

[81] Ahmed Al-Rawi: Cyber Warriors in the Middle East: The Case of the Syrian Electronic Army. *Public Relations Review,* 40, no. 3 (2014). 420.

2015 proposed a set of norms that was later endorsed by the G20. The success of the UNGGE was great, but even so, it could not agree to its 2017 report, suggesting deep dissent. The UN Secretary-General, and other respected private and public entities, may also work on facilitating Track 1.5 and Track 2 dialogues. These are efforts that engage government and industry in discussions on cybersecurity outside the formal constraints of multilateral interactions. There is also an open ended working group that studies this, and numerous other UN institutions, but other chapters in this work detail those more. Suffice to say, that at first blush, why the UN is such a large actor in the cyber diplomatic world, is because the "legality of cyberattacks is generally approached from the use of force prohibition contained in Article 2(4) UN Charter".[82]

Conclusion

As we have seen in this review of the literature, there is a growing consensus that cyber diplomacy deserves a study on its own. The evolution of the literature clearly demonstrates conceptual advances, distinguishing between cyber diplomacy and digital diplomacy. It is also clear that the initial literature on cyber diplomacy follows the traditional international relations paradigms, and can be grouped around realist, liberal and constructivist thinking. The United Nations, as an independent actor and also as a forum for intergovernmental rule and norm setting, deserves separate studies, which is not part of this literature review. Its role will most likely be extremely important in the future of cyber diplomacy.

At the state level, even for an organisation as powerful as the U.S. Government, the cyber realm brings with it notable challenges and issues. When it comes to the military, it must realise that "cyber operations do not fit neatly into this paradigm because although they are 'non-forceful' (that is, non-kinetic), their consequences can range from mere annoyance to death".[83] And when it comes to cyber diplomacy, the State Department and policy makers must understand that "there is no international consensus on a precise definition of a use of force, in or out of cyberspace".[84]

[82] Buchan (2012): op. cit. 211.

[83] Michael N. Schmitt: Cyber Operations and the Jus Ad Bellum Revisited. *Villanova Law Review,* 56, no. 3 (2011). 573.

[84] Ibid.

Finally, what this literature review only touched upon due to space constraints, is the role of non-governmental organisations and individuals. How does civil society fit into the world of cyber diplomacy? Who and when will challenge the supremacy of the state as an actor in the world of cyber diplomacy? Does the problem of attribution hinder or accelerate this process? These are all questions that future research must answer as we determine where we go from here.

References

Abomhara, Mohamed – Geir M. Køien: Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *Journal of Cyber Security and Mobility,* 4, no. 1 (2015). 65–88. Online: https://doi.org/10.13052/jcsm2245-1439.414

Al-Rawi, Ahmed: Cyber Warriors in the Middle East: The Case of the Syrian Electronic Army. *Public Relations Review,* 40, no. 3 (2014). 420–428. Online: https://doi.org/10.1016/j.pubrev.2014.04.005

Awan, Imran: Cyber-Extremism: Isis and the Power of Social Media. *Society,* 54, no. 2 (2017). 138–149. Online: https://doi.org/10.1007/s12115-017-0114-0

Barford, Paul – Marc Dacier – Thomas G. Dietterich – Matt Fredrikson – Jon Giffin – Sushil Jajodia – Somesh Jha – Peng Liu – Peng Ning – Xinming Ou – Dawn Song – Laura Strater – Vipin Swarup – George Tadda – Cliff Wang – John Yen: Cyber SA: Situational Awareness for Cyber Defense. In Sushil Jajodia – Peng Liu – Vipin Swarup and CLiff Wang (eds.): *Cyber Situational Awareness: Issues and Research.* Boston, Mass., Springer, 2010. 3–13. Online: https://doi.org/10.1007/978-1-4419-0140-8_1

Barnard-Wills, David – Debi Ashenden: Securing Virtual Space: Cyber War, Cyber Terror, and Risk. *Space and Culture,* 15, no. 2 (2012). 110–123. Online: https://doi.org/10.1177/1206331211430016

Barrinha, André – Thomas Renard: Cyber-diplomacy: The Making of an International Society in the Digital Age. *Journal of Global Affairs,* 3, nos. 4–5 (2017). 353–364. Online: https://doi.org/10.1080/23340460.2017.1414924

Betts, Richard K.: The Soft Underbelly of American Primacy: Tactical Advantages of Terror. *Political Science Quarterly,* 117, no. 1 (2002). 19–36. Online: https://doi.org/10.2307/798092

Buchan, Russell: Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? *Journal of Conflict and Security Law,* 17, no. 2 (2012). 212–227. Online: https://doi.org/10.1093/jcsl/krs014

Brunst, Phillip W.: Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet. In Marianne Wade – Almir Maljevic (eds.): *A War on Terror?* New York, Springer, 2010. 51–78. Online: https://doi.org/10.1007/978-0-387-89291-7

Cavelty, Myriam Dunn: *The Militarisation of Cyberspace: Why Less May Be Better.* Tallinn, NATO CCD COE Publications, 2012.

Clark, Richard A. – Robert K. Knake: *Cyber War: The Next Threat to National Security and What to Do About It.* New York, Harper Collins, 2010.

CCDCOE: *The Tallin Manual.* 2017. Online: https://ccdcoe.org/research/tallinn-manual/

Chen, Yu – Kai Hwang – Wei-Shinn Ku: Collaborative Detection of DDoS Attacks over Multiple Network Domains. *IEEE Transactions on Parallel and Distributed Systems,* 18, no. 12 (2007). 1649–1662. Online: https://doi.org/10.1109/TPDS.2007.1111

Cull, Nicholas J.: Public Diplomacy: Seven Lessons for Its Future from Its Past. *Place Branding and Public Diplomacy,* 6, no. 1 (2010). 11–17. Online: https://doi.org/10.1057/pb.2010.4

Cyber Peace Alliance: *Cyber Diplomacy: Governance Beyond Government.* 12 October 2019. Online: https://medium.com/@cyberdiplomacy/cyber-diplomacy-governance-beyond-government-e8b92efff8f

D'Amico, Anita – Kristen Whitley – Daniel Tesone – Brianne O'Brien – Emilie Roth: Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts. *Proceedings of the Human Factors and Ergonomics Society,* 49, no. 3 (2005). 229–233. Online: https://doi.org/10.1177/154193120504900304

De Bruijn, Hans – Marijn Janssen: Building Cybersecurity Awareness: The Need for Evidence-based Framing Strategies. *Government Information Quarterly,* 34, no. 1 (2017). 1–7. Online: https://doi.org/10.1016/j.giq.2017.02.007

Deibert, Ronald J. – Rafal Rohozinski – Masashi Crete-Nishihata: Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War. *Security Dialogue,* 43, no. 1 (2012). 3–24. Online: https://doi.org/10.1177/0967010611431079

Denning, Dorothy E.: Framework and Principles for Active Cyber Defense. *Computers and Security,* 40 (2014). 108–113. Online: https://doi.org/10.1016/j.cose.2013.11.004

Dinstein, Yoram: The Principle of Distinction and Cyber War in International Armed Conflicts. *Journal of Conflict and Security Law,* 17, no. 2 (2012). 261–277. Online: https://doi.org/10.1093/jcsl/krs015

Droege, Cordula: Get Off my Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians. *International Review of the Red Cross,* 94, no. 886 (2012). 533–578. Online: https://doi.org/10.1017/S1816383113000246

Elliott, David: Deterring Strategic Cyberattack. *IEEE Security and Privacy,* 9, no. 5 (2011). 36–40. Online: https://doi.org/10.1109/MSP.2011.24

Eom, Jung-Ho – Nam-Uk Kim – Shung-Hwan Kim – Tai-Myoung Chung: Cyber Military Strategy for Cyberspace Superiority in Cyber Warfare. In *2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec).* IEEE. Online: https://doi.org/10.1109/CyberSec.2012.6246114

Farwell, James P. – Rafal Rohozinski: Stuxnet and the Future of Cyber War. *Survival,* 53, no. 1 (2011). 23–40. Online: https://doi.org/10.1080/00396338.2011.555586

Farwell, James P. – Rafal Rohozinski: The New Reality of Cyber War. *Survival,* 54, no. 4 (2012). 107–120. Online: https://doi.org/10.1080/00396338.2012.709391

Fung, Brian: How Many Cyberattacks Hit the United States Last Year? *Nextgov,* 08 March 2013. Online: www.nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/

Geers, Kenneth: The Challenge of Cyber Attack Deterrence. *Computer Law and Security Review,* 26, no 3 (2010). 298–303. Online: https://doi.org/10.1016/j.clsr.2010.03.003

Gjelten, Tom: Shadow Wars: Debating Cyber 'Disarmament'. *World Affairs,* 173, no. 33 (2010). 33–42.

Golling, Mario – Björn Stelte: Requirements for a Future EWS – Cyber Defence in the Internet of the Future. In *2011 3rd International Conference on Cyber Conflict.* IEEE.

Gutzwiller, Robert S. – Sunny Fugate – Benjamin D. Sawyer – P. A. Hancock: The Human Factors of Cyber Network Defense. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting,* 59, no. 1 (2015). 322–326. Online: https://doi.org/10.1177/1541931215591067

Hausken, Kjell: Income, Interdependence, and Substitution Effects Affecting Incentives for Security Investment. *Journal of Accounting and Public Policy,* 25, no. 6 (2006). 629–665. Online: https://doi.org/10.1016/j.jaccpubpol.2006.09.001

Hausken, Kjell: Information Sharing among Firms and Cyber Attacks. *Journal of Accounting and Public Policy,* 26, no. 6 (2007). 639–688. Online: https://doi.org/10.1016/j.jaccpubpol.2007.10.001

Healey, Jason – Neil Jenkins: Rough-and-Ready: A Policy Framework to Determine if Cyber Deterrence is Working or Failing. In Tomáš Minárik – Siim Alatalu – Stefano Biondi – Massimiliano Signoretti – Ihsan Tolga – Gábor Visky (eds.): *11th International Conference on Cyber Conflict: Silent Battle.* Tallinn, NATO CCD COE Publications, 2019. 123–142.

Heckman, Kristin E. – Michael J. Walsh – Frank J. Stech – Todd A. O'Boyle – Stephen R. DiCato – Audra F. Herber: Active Cyber Defense with Denial and Deception: A Cyber-wargame Experiment. *Computers and Security,* 37. (2013). 72–77. Online: https://doi.org/10.1016/j.cose.2013.03.015

Hernandez-Ardieta, Jorge L. – Juan E. Tapiador – Guillermo Suarez-Tangil: Information Sharing Models for Cooperative Cyber Defence. In *2013 5th International Conference on Cyber Conflict (CYCON 2013).* IEEE.

Herrington, Lewis – Richard Aldrich: The Future of Cyber-Resilience in an Age of Global Complexity. *Politics,* 33, no. 4 (2013). 299–310. Online: https://doi.org/10.1111/1467-9256.12035

Hua, Jian – Sanjay Bapna: The Economic Impact of Cyber Terrorism. *The Journal of Strategic Information Systems,* 22, no. 2 (2013). 175–186. Online: https://doi.org/10.1016/j.jsis.2012.10.004

Jabbour, Kamaal T. – Paul E. Ratazzi: Does the United States Need a New Model for Cyber Deterrence? In Adam B. Lowther (ed.): *Deterrence.* New York, Palgrave Macmillan, 2012. Online: https://doi.org/10.1057/9781137289810_3

Junio, Timothy J.: How Probable Is Cyber War? Bringing IR Theory Back In to The Cyber Conflict. *Journal of Strategic Studies,* 36, no. 1 (2013). 125–133. Online: https://doi.org/10.1080/01402390.2012.739561

Knapp, Kenneth J. – William R. Boulton: Cyber-Warfare Threatens Corporations: Expansion into Commercial Environments. *Information Systems Management,* 23, no. 2 (2006). 76–87. Online: https://doi.org/10.1201/1078.10580530/45925.23.2.20060301/92675.8

Konkel, Frank R.: Pentagon Thwarts 36 Million Email Breach Attempts Daily. *Nextgov,* 11 January 2018. Online: www.nextgov.com/cybersecurity/2018/01/pentagon-thwarts-36-million-email-breach-attempts-daily/145149/

Kotenko, Igor: Agent-based Modeling and Simulation of Cyber-warfare between Malefactors and Security Agents. In *19th European Conference on Modelling and Simulation.* ECMS, 2005.

Khsetri, Nir: Pattern of Global Cyber War and Crime: A Conceptual Framework. *Journal of International Management,* 11, no. 4 (2005). 541–562. Online: https://doi.org/10.1016/j.intman.2005.09.009

Kurbalija, Jovan: *An Introduction to Internet Governance.* Msida–Geneva, DiploFoundation, 2016.

Lawson, Sean: Putting the "War" in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States. *First Monday,* 17, no. 7 (2012). Online: https://doi.org/10.5210/fm.v17i7.3848

Liff, Adam P.: Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies,* 35, no. 3 (2012). 134–138. Online: https://doi.org/10.1080/01402390.2012.663252

Lindsay, Jon R.: The Impact of China on Cybersecurity: Fiction and Friction. *International Security,* 39, no. 3 (2015). 7–47.

Lindsay, Jon R.: Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack. *Journal of Cybersecurity,* 1, no. 1 (2015). 53–67. Online: https://doi.org/10.1093/cybsec/tyv003

Liu, Peng – Wanyu Zang: Incentive-Based Modeling and Inference of Attacker Intent, Objectives, and Strategies. *ACM Transactions on Information and System Security (TISSEC),* 8, no. 1 (2005). 78–118.

Lucas, George R. Jr.: Postmodern War. *Journal of Military Ethics,* 9, no. 4 (2010). 289–298. Online: https://doi.org/10.1080/15027570.2010.536399

Lynn, William J. III: Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs,* 89, no. 5 (2010). 97–108.

McGraw, Gary: Cyber War Is Inevitable (Unless We Build Security In). *Journal of Strategic Studies,* 36, no. 1 (2013). 109–119. Online: https://doi.org/10.1080/01402390.2012.742013

McQueen, Miles A. – Wayne F. Boyer: Deception Used for Cyber Defense of Control Systems. In *2009 2nd Conference on Human System Interactions.* IEEE. 624–631. Online: https://doi.org/10.1109/HSI.2009.5091050

Mullins, Barry E. – Timothy H. Lacey – Robert F. Mills – Joseph M. Trechter – Samuel D. Bass: How the Cyber Defense Exercise Shaped an Information-Assurance Curriculum. *IEEE Security and Privacy Magazine,* 5, no. 5 (2007). 40–49. Online: https://doi.org/10.1109/MSP.2007.111

Mureşan, Radu Constantin: Current Approaches of Diplomacy in the Cyberspace. *Studia Universitatis Babeş-Bolyai,* 62, no. 2 (2017). 31–44. Online: https://doi.org/10.24193/subbeuropaea.2017.2.03

Nazir, Sajid – Shushma Patel – Dilip Patel: Assessing and Augmenting SCADA Cyber Security: A Survey of Techniques. *Computers and Security,* 70 (2017). 436–454. Online: https://doi.org/10.1016/j.cose.2017.06.010

North Atlantic Treaty Organization: *Cyber Defence Pledge.* 08 July 2016. Online: www.nato.int/cps/en/natohq/official_texts_133177.htm

North Atlantic Treaty Organization: *Press Conference by NATO Secretary General Jens Stoltenberg Following the Meeting of NATO Ministers of Foreign Affairs.* 02 April 2020. Online: www.nato.int/cps/en/natohq/opinions_174772.htm

North Atlantic Treaty Organization: *The North Atlantic Treaty. Washington D.C. – 4 April 1949.* 10 April 2019. Online: www.nato.int/cps/en/natolive/official_texts_17120.htm

Nye, Joseph S. Jr.: Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly,* 5, no. 4 (2011a). 18–38.

Nye, Joseph S. Jr.: *The Future of Power.* New York, PublicAffairs, 2011b.

Nye, Joseph S. Jr.: Deterrence and Dissuasion in Cyberspace. *International Security,* 41, no. 3 (2016). 44–71. Online: https://doi.org/10.1162/ISEC_a_00266

Nye, Joseph S. Jr.: How Will New Cybersecurity Norms Develop? *Project Syndicate,* 08 March 2018. Online: www.project-syndicate.org/commentary/origin-of-new-cybersecurity-norms-by-joseph-s--nye-2018-03

O'Connell, Mary Ellen: Cybersecurity Without Cyber War. *Journal of Conflict and Security Law,* 17, no. 2 (2012). 187–209. Online: https://doi.org/10.1093/jcsl/krs017
Power, Marcus: Video War Games and Post 9/11 Cyber-deterrence. *Security Dialogue,* 38, no. 2 (2007). 221–288. Online: https://doi.org/10.1177/0967010607078552
Powers, Shawn – Michael Jablonski: *The Real Cyber War. The Political Economy of Internet Freedom.* Champaign, IL, University of Illinois Press, 2015.
Rid, Thomas: Cyber War Will Not Take Place. *Journal of Strategic Studies,* 35, no. 1 (2012). 5–32. Online: https://doi.org/10.1080/01402390.2011.608939
Robinson, Michael – Kevin Jones – Helge Janicke: Cyber Warfare: Issues and Challenges. *Computers and Security,* 49 (2015). 70–94. Online: https://doi.org/10.1016/j.cose.2014.11.007
Sagan, Scott – Kenneth Waltz – Richard K. Betts: A Nuclear Iran: Promoting Stability or Courting Disaster? *Journal of International Affairs,* 60, no. 2 (2007). 135–150.
Sangster, Benjamin – T. J. O'Connor – Thomas Cook – Robert Fanelli – Erik Dean – William J. Adams – Chris Morrell – Gregory Conti: *Toward Instrumenting Network Warfare Competitions to Generate Labeled Datasets.* United States Military Academy, 2nd Workshop on Cyber Security Experimentation and Test, 2009.
Schmitt, Michael N.: Cyber Operations and the Jus Ad Bellum Revisited. *Villanova Law Review,* 56, no. 3 (2011). 569–579.
Schreiber-Ehle, Sabine – Johann Wolfgang Koch: The JDL Model of Data Fusion Applied to Cyber-defence – A Review Paper. In *2012 Workshop on Sensor Data Fusion: Trends, Solutions, Applications, (SDF).* IEEE. 116–119. Online: https://doi.org/10.1109/SDF.2012.6327919
Sharma, Amit: Cyber Wars: A Paradigm Shift from Means to Ends. *Strategic Analysis,* 34, no. 1 (2010). 62–73. Online: https://doi.org/10.1080/09700160903354450
Sharp, Travis: Theorizing Cyber Coercion: The 2014 North Korean Operation against Sony. *Journal of Strategic Studies,* 40, no. 7 (2017). 898–926. Online: https://doi.org/10.1080/01402390.2017.1307741
Skopik, Florian – Giuseppe Settanni – Roman Fiedler: A Problem Shared Is a Problem Halved: A Survey on the Dimensions of Collective Cyber Defense through Security Information Sharing. *Computers and Security,* 60 (2016). 154–176. Online: https://doi.org/10.1016/j.cose.2016.04.003
Sridhar, Siddharth – Manimaran Govindarasu: Model-Based Attack Detection and Mitigation for Automatic Generation Control. *IEEE Transactions on Smart Grid,* 5, no. 2 (2014). 580–591. Online: https://doi.org/10.1109/TSG.2014.2298195
Stone, John: Cyber War *Will* Take Place! *Journal of Strategic Studies,* 36, no. 1 (2013). 101–108. Online: https://doi.org/10.1080/01402390.2012.730485
Taddeo, Mariarosaria: The Limits of Deterrence Theory in Cyberspace. *Philosophy and Technology,* 31, no. 3 (2018). 339–355. Online: https://doi.org/10.1007/s13347-017-0290-2
The White House: *Statement from the Press Secretary.* 15 February 2018. Online: https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/
Tor, Uri: 'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence. *Journal of Strategic Studies,* 40, nos. 1–2 (2015). 92–117. Online: https://doi.org/10.1080/01402390.2015.1115975
Turns, David: Cyber Warfare and the Notion of Direct Participation in Hostilities. *Journal of Conflict and Security Law,* 17, no. 2 (2012). 279–297. Online: https://doi.org/10.1093/jcsl/krs021
Uma, M. – Padmavathi Ganapathi: A Survey on Various Cyber Attacks and their Classification. *International Journal of Network Security,* 15, no. 5 (2013). 390–396.

U.S. Department of State: *Office of the Coordinator for Cyber Issues.* 2020. Online: www.state.gov/bureaus-offices/secretary-of-state/office-of-the-coordinator-for-cyber-issues/

U.S. Department of Treasury: *Treasury Sanctions Russian Federal Security Service Enablers.* 11 June 2018. Online: https://home.treasury.gov/news/press-releases/sm0410

Valeriano, Brandon – Ryan C. Maness: *Cyber War versus Cyber Realities. Cyber Conflict in the International System.* New York, Oxford University Press, 2015. Online: https://doi.org/10.1093/acprof:oso/9780190204792.001.0001

Walker-Roberts, Steven – Mohammad Hammoudeh – Ali Dehghantana: A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure. *IEEE Access,* 6 (2018). 25167–25177. Online: https://doi.org/10.1109/ACCESS.2018.2817560

World Summit on the Information Society: *Declaration of Principles.* 12 December 2003. Online: www.itu.int/net/wsis/docs/geneva/official/dop.html

Yu, Jia – Kui Ren – Chong Wang: Enabling Cloud Storage Auditing with Verifiable Outsourcing of Key Updates. *IEEE Transactions on Information Forensics and Security,* 11, no. 6 (2016). 1362–1375. Online: https://doi.org/10.1109/TIFS.2016.2528500

Anna Molnár

European Union – Cybersecurity

Introduction

It is a commonplace to state that European societies, governmental and private sectors are increasingly dependent on digital technologies. Electronic networks and information systems have developed to be part of our daily lives. In recent years, digital technology has become an essential tool on which not only all sectors of the economy, but also every area of our lives rely. Highlighting only a few of them, such as electricity or transport networks, production and financial processes, and health care systems, a significant degree of interdependence and interconnection can be observed.

As a result, the European economies, governmental or defence infrastructures, and in this context, even the functioning of democracy, European values and liberties can be threatened by malicious cyber activities. Europe's security largely depends on the cyber resilience of Member States and EU institutions: the ability to prepare for and to respond to the ever-changing and growing intensity of cyber threats. Today, many business models rely on the smooth operation of the Internet and information systems. In parallel, the economic impact of cybercrime is steadily increasing. In addition to racketeering, many other threats are a major challenge for European economic and political actors. In today's computer age, the protection of personal data also plays a crucial role in the implementation of cybersecurity.

The widely used term of cybersecurity is not limited to network and information security in the policy circles of the EU. According to a report prepared by the European Court of Auditors, the cybersecurity ecosystem includes any illegal activity realised by the use of digital technologies in cyberspace. It refers to cybercrimes like computer virus attacks and non-cash payment fraud, and the dissemination of online child sexual abuse material. It includes disinformation campaigns to influence online debate and suspected electoral interference. According to the definition of Europol, a connection between cybercrime and

https://doi.org/10.36250/01039_02

terrorism can be observed.[1] Not only government institutions, but also European Internet users and companies have experienced several cybersecurity incidents. It is crucial to guarantee that devices and networks are protected to deter cyber-attacks. Despite the fact that the European Union has started to strengthen its comprehensive cybersecurity governance, an analysis prepared by the European Court of Auditors has highlighted several weaknesses and shortfalls in the governance and in the legislative framework in 2019. The complex ecosystem of the EU's cybersecurity policy is closely linked to internal policy areas; regarding internal policy areas, it covers justice and home affairs, the digital single market and research policies as well. The EU has become increasingly active in external policy areas as well, and cybersecurity is closely linked to diplomacy, and to security and defence policy.[2]

The Strategic Framework and Regulations of the European Union

The Strategic Framework since 2000

The EU has been an observer organisation to the Cybercrime Convention Committee of the Council of Europe since 2001 (the Budapest Convention), which provided a framework for the promotion of international cooperation and legislation against cybercrime. Despite the growing awareness, the threats and challenges related to cybersecurity were only briefly mentioned by the strategies of the EU during the first decade of the 21st century. In 2003, the European Security Strategy already implicitly referred to cybersecurity. The document developed by Javier Solana, High Representative for the Common Foreign and Security Policy, only highlighted the danger of terrorist movements connected by electronic networks.[3] In 2005, the European Commission published a comprehensive strategy entitled *i2010: A European Information Society for Growth and Employment.* The new strategy aimed to promote the development of an open and competitive digital economy and emphasised the key role of ICT (information and communication

[1] European Court of Auditors (2019): Challenges to Effective EU Cybersecurity Policy. *Briefing Paper,* March 2019. 6.

[2] European Court of Auditors (2019): op. cit. 12.

[3] Council of the European Union: *European Security Strategy. A Secure Europe in a Better World.* Brussels, General Secretariat of the Council, 2009. 30.

technology) in social inclusion and quality of life. The document mentions the issue of security in many cases. In the interest of a secure and reliable ICT, the European Commission articulated the need to develop a Strategy for a Secure Information Society.[4]

Additionally, the 2008 review of the European Security Strategy has already addressed the basic issues of cybersecurity in a short section. The document emphasised that modern economies are highly dependent on critical infrastructure such as the Internet. Internet-based crime was mentioned in the Strategy for a Secure European Information Society, adopted in 2006. However, as a result of attacks on governments of Member States or private IT systems, a new dimension related to a potential new economic, political and military weapon was added. The document underlined the need for more work to explore a comprehensive EU approach, raise awareness and enhance international cooperation.[5] The Internal Security Strategy of the European Union, adopted in 2010, drew attention to the dangers of cybercrime in the Union.[6]

In May 2010, after the Lisbon Strategy, the European Commission launched the *Europe 2020 Strategy,* which aimed at reducing vulnerability and increasing competitiveness.[7] As one of the flagship initiatives of the new strategy, the European Commission has launched the *Digital Agenda for Europe (DAE).* The agenda aimed to make the use of information and communication technologies (ICT) a key factor in achieving the goals set in the *Europe 2020 Strategy.* The European Commission has built the *Digital Single Market Strategy* on three pillars to ensure a fair, open and secure digital environment: (1) Ensuring better access to digital goods and services for consumers and businesses across Europe; (2) Creating the right conditions for digital networks and services; and (3) Maximising the growth potential of the digital economy.[8]

[4] European Commission: Brussels, 1.6.2005, COM(2005) 229 final, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions "i2010 – A European Information Society for Growth and Employment". Commission of the European Communities, 2005.

[5] Council of the European Union: *Report on the Implementation of the European Security Strategy. Providing Security in a Changing World.* Brussels, 11 December 2008. 5.

[6] Council of the European Union: *Internal Security Strategy for the European Union. Towards a European Security Model.* Brussels, General Secretariat of the Council, 2010. 7.

[7] László Kovács: *Kiberbiztonság és stratégia.* Budapest, Dialóg Campus, 2018. 85.

[8] European Commission: *Shaping the Digital Single Market.* 2020.

In particular, the EU intended to respond adequately to challenges in the digital domain, such as the fragmentation of the digital market, interoperability issues, the very rapid spread of cybercrime, the low level of R&D and investment in it, or the low level of digital literacy in many regions of the EU.[9]

Table 1. *Strategy Papers of the European Union on Cybersecurity*

Year	Strategy Papers of the European Union
2003	European Security Strategy
2005	i2010: European Information Society for Growth and Employment
2006	Strategy for a Secure European Information Society
2008	Report on the Implementation of the European Security Strategy. Providing Security in a Changing World
2010	Internal Security Strategy for the European Union. Towards a European Security Model
2010	A Digital Agenda for Europe
2013	Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace
2014	EU Cyber Defence Policy Framework
2015	Council Conclusions on Cyber Diplomacy
2015	Digital Single Market Strategy for Europe
2016	Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy
2017	Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU
2018	EU Cyber Defence Policy Framework
2020	The EU's Cybersecurity Strategy for the Digital Decade
2021–2027	Digital Europe Programme (DIGITAL)

Source: Compiled by the author based on Rehrl (2018): op. cit. 26.

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013)

The EU began developing its first comprehensive cybersecurity strategy in 2012–2013. All of this happened at a time when developed countries were realising the strategic importance of cybersecurity challenges. Compared to NATO, whose

[9] Kovács (2018): op. cit. 86.

first strategies (2008, 2011) focused solely on protecting its own IT network, the first EU strategy covered almost all areas of EU competences.[10]

Following the entry into force of the Lisbon Treaty, the European External Action Service and the European Commission, under the leadership of EU High Representative for Foreign Affairs and Security Policy Catherine Ashton, also worked together to draft the joint communication. In 2013 the *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* was adopted by the European External Action Service and the European Commission. This document first mentioned the need for a coherent EU international cyberspace policy and cyber defence objectives. One of the main goals and principles of the strategy was to uphold EU core values and promote a peaceful, open and transparent use of cyber technologies.[11]

The implementation of the strategy was primarily the responsibility of some Directorates-General of the European Commission. The Directorate-General for Content, Technology and Communication Networks (DG CNETC) was responsible for legislation, industrial policy and research and development in the new cyber areas. The Directorate-General for Migration and EU Home Affairs (DG HOME) has been responsible for shaping cyber law enforcement policy and promoting cooperation between Member States in this area.

The principles set out in the strategy were in line with the general principles and values of the EU: (1) The core values of the European Union apply to the digital world as much as to the physical world; (2) Protection of fundamental rights, freedom of expression, personal data and privacy; (3) Access for all; (4) Democratic and efficient multi-stakeholder governance; (5) Shared responsibility to ensure security.

However, the strategy sets out five priorities: (1) Achieving resilience to cyberattacks; (2) A drastic reduction in cybercrime; (3) Developing cyber defence policy and capabilities for the Common Security and Defence Policy (CSDP); (4) Development of cybersecurity industry and technological resources; (5) Establishing a coherent international policy on cyberspace for the European Union and promoting the Union's core values.[12]

[10] Jochen Rehrl (ed.): *Handbook on Cybersecurity. The Common Security and Defence Policy of the European Union.* Luxembourg Publications Office of the European Union, 2018. 18.

[11] European Commission: *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* JOIN/2013/01 final.

[12] Ibid.

EU Cyber Defence Policy Framework (2014)

The European External Action Service (EEAS) is responsible for promoting cyber defence activities and developing international cyber policy goals including cyber diplomacy and strategic communication, and hosts intelligence and analysis centres.[13] According to the European Council Conclusions on CSDP in December 2013, the cyber defence policy framework was developed by the EEAS together with the European Commission and the European Defence Agency.[14] Under the leadership of the EEAS, the EU Cyber Defence Policy Framework was completed in 2014.

The document established the following objectives:

1. Supporting the development of cyber defence capabilities of Member States in areas related to the common security and defence policy
2. Enhancing the protection of communication and information networks used by the EEAS in the field of CSDP
3. Promoting civil–military cooperation and synergies with the wider EU cyber policies to address the new challenges
4. Help cooperation with the private sector on cyber defence capability development
5. Improving training, education and exercise opportunities
6. Enhancing cooperation with relevant international partners, in particular with NATO[15]

Directive on the Security of Network and Information Systems (2016)

The European Union adopted the first EU-wide legislation on cybersecurity in 2016 with the Directive (EU) 2016/1148 of the European Parliament and the Council on the security of network and information systems (NIS). The NIS Directive had to be transposed into national laws of the EU Member States

[13] European Court of Auditors (2019): op. cit. 10.

[14] European Council: *European Council Conclusions 19/21 December 2013.*

[15] Council of the European Union: *EU Cyber Defence Policy Framework.* Brussels, 18 November 2014.

by 9 May 2018 and the units providing essential services had to be identified by 9 November 2018.

The aim of the NIS Directive is to introduce comprehensive measures that can increase the level of security of network and information systems and services which play a vital role in the economy and society of the Union. Implementing the directive will enable EU countries to prepare for and respond to cyberattacks. To this end, it has become necessary at Member State level to (1) designate competent authorities; (2) set up Computer Security Incident Response teams (CSIRTs); and (3) adopt national cybersecurity strategies. The measures introduced will strengthen cooperation at both strategic and technical levels in the European Union.[16]

However, the Directive obliges essential and digital service providers (such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructures) to take appropriate security measures and to inform the relevant national authorities of serious incidents.

Under the new rules, EU Member States must also adopt national cybersecurity strategies for network and information systems. Strategies at the national level should include the following issues:

> "(a) the objectives and priorities of the national strategy on the security of network and information systems;
> (b) a governance framework to achieve the objectives and priorities of the national strategy on the security of network and information systems, including roles and responsibilities of the government bodies and the other relevant actors;
> (c) the identification of measures relating to preparedness, response and recovery, including cooperation between the public and private sectors;
> (d) an indication of the education, awareness-raising and training programmes relating to the national strategy on the security of network and information systems;
> (e) an indication of the research and development plans relating to the national strategy on the security of network and information systems;
> (f) a risk assessment plan to identify risks;
> (g) a list of the various actors involved in the implementation of the national strategy on the security of network and information systems.
>
> It is the responsibility of the national competent authorities to monitor the application of the Directive. To this end, national authorities should assess the level of security of network and information systems. They should also participate in the work of the Cooperation

[16] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union.

> Group, which is composed of representatives of the Member States, the Commission and European Commission and the European Network and Information Security Agency (ENISA). The national competent authorities shall inform the public about individual incidents where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident."[17]

Global Strategy (2016)

The European Union's Global Strategy for Foreign and Security Policy (hereinafter referred to as the Global Strategy), adopted in 2016, has already addressed the issue of cybersecurity in details. The strategy calls for the strengthening of the EU as a security community and the development of capabilities for the protection of EU citizens and the response to external crises. In addition, the interoperability of civilian and military capabilities needs to be strengthened.

The Global Strategy emphasises that the Union will focus on cybersecurity in the future and will be able to respond more effectively to cyber threats. With this new strategy, the EU intended to address open, free and secure cyberspace in all policy areas.[18]

> "The EU will increase its focus on cyber security, equipping the EU and assisting Member States in protecting themselves against cyber threats while maintaining an open, free and safe cyberspace. This entails strengthening the technological capabilities aimed at mitigating threats and the resilience of critical infrastructure, networks and services, and reducing cybercrime. It means fostering innovative information and communication technology (ICT) systems which guarantee the availability and integrity of data, while ensuring security within the European digital space through appropriate policies on the location of data storage and the certification of digital products and services. It requires weaving cyber issues across all policy areas, reinforcing the cyber elements in CSDP missions and operations, and further developing platforms for cooperation. The EU will support political, operational and technical cyber cooperation between Member States, notably on analysis and consequence management, and foster shared assessments between EU structures and the relevant institutions in Member States. It will enhance its cyber security cooperation with core partners such as the US and NATO. The EU's response will also be embedded in strong public-private partnerships. Cooperation and information-sharing between Member States, institutions, the private sector and civil society can foster a common cyber security culture, and raise preparedness for possible cyber disruptions and attacks."[19]

[17] Directive (EU) 2016/1148.

[18] European External Action Service: *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy.* 2016.

[19] Ibid. 21–22.

Review of the Cyber Security Strategy (2017)

As the goals set in the 2013 cybersecurity strategy were not always met and changes in cybersecurity threats have taken place to such an extent in recent years, it has become inevitable to review the first strategy and develop a new one. Disruptive computer operations against critical infrastructures, democratic institutions and the Internet of Things (IoT), as well as large-scale botnet attacks and global ransomware infections such as "WannaCry" and "NotPetya") drew attention to cyber risks and the need for proactive action at EU level.[20]

Under the leadership of the European Commission, the revision of the EU cybersecurity strategy was completed in 2017. The joint communication from the EC and the High Representative for Foreign Affairs and Security Policy to the European Parliament and the Council was entitled *Resilience, Deterrence, Defence: Building Strong Cybersecurity for the EU.*[21]

The strategy highlights as follows:

> "Cybersecurity is critical to both our prosperity and our security. As our daily lives and economies become increasingly dependent on digital technologies, we become more and more exposed. Cybersecurity incidents are diversifying both in terms of who is responsible and what they seek to achieve. Malicious cyber activities not only threaten our economies and the drive to the Digital Single Market, but also the very functioning of our democracies, our freedoms and our values. Our future security depends on transforming our ability to protect the EU against cyber threats: both civilian infrastructure and military capacity rely on secure digital systems. This has been recognised by the June 2017 European Council, as well as in the Global Strategy on Foreign and Security Policy for the European Union."[22]

The document underlines that:

> "While Member States remain responsible for national security, the scale and cross-border nature of the threat make a powerful case for EU action providing incentives and support for Member States to develop and maintain more and better national cybersecurity capabilities, while at the same time building EU-level capacity."[23]

[20] Rehrl (2018): op. cit. 23.

[21] European Commission: *Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU.* Brussels, 13.9.2017, JOIN(2017) 450 final.

[22] Ibid.

[23] Ibid.

The new strategy proposed new measures to ensure the EU's resilience, deterrence and protection against cyberattacks. These proposals included the strengthening of the European Network and Information Security Agency (ENISA), the development of a voluntary EU cybersecurity certification framework to enhance the cybersecurity of digital products and services, and a plan for rapid, coordinated response to large-scale cybersecurity incidents and crises. The Commission proposed a permanent mandate for the ENISA, which, having a strong advisory role on policy development and implementation, will support Member States, EU institutions and businesses in key areas. The joint communication highlights cyber defence as a priority for EU actions. According to the document, the 2014 EU cyber defence policy framework needed to be renewed.[24]

The 2017 Cybersecurity Package and the Digital Single Market Strategy

In September 2017, in his annual speech at the European Parliament (State of the Union), President Jean-Claude Juncker highlighted the importance of the progress during the previous three years in keeping Europeans safe online. But he also stated that Europe was not well prepared against cyberattacks. Jean-Claude Juncker argued strongly in favour of establishing new tools against cyberattacks, such as the European Cybersecurity Agency. The European Commission and the High Representative proposed a Cybersecurity Package, a wide-ranging set of measures to strengthen cybersecurity in the EU. This included a proposal for an EU Cybersecurity Agency, a new EU-wide certification framework for products and services in the digital world, organisation of yearly pan-European cybersecurity exercises. According to Federica Mogherini, High Representative of the Union, the EU is developing an international cyber policy supporting an open, free and secure cyberspace. It also promotes all efforts in order to establish "norms of responsible state behaviour, apply international law and confidence building measures in cybersecurity".[25]

[24] Ibid.

[25] European Commission: *State of the Union 2017 – Cybersecurity: Commission Scales Up EU's Response to Cyber-attacks.* Brussels, 19 September 2017.

Cybersecurity Act

As part of the cybersecurity package adopted in September 2017, the realisation of a new legislation on cybersecurity (known as the Cybersecurity Act), which is one of the priorities of the Digital Single Market Strategy, has begun. In September 2018, the European Commission proposed the establishment of a European Cybersecurity Industrial, Technology and Research Competence Centre and a network of cybersecurity competence centres.[26]

The priority of the Digital Single Market Strategy (2015) was to remove barriers to online transactions and provide consumers with secure access to products and services.[27] The new European Cybersecurity Act was proposed in 2017 and was adopted in 2019 by the European Parliament and the Council. The new legislation covered the following areas: setting the new mandate of ENISA, the EU Agency for Cybersecurity and establishing the European cybersecurity certification framework. ENISA will support Member States in effective response to cyberattacks in the new cybersecurity certification framework. With the entry into force of the Cybersecurity Act, the ENISA, the EU Agency for Cybersecurity will have a permanent mandate, strengthened responsibilities and increased resources.[28]

Cyber Defence and Permanent Structured Cooperation (PESCO)

From 2017, the process of implementing the permanent structured cooperation (PESCO) provided by the Lisbon Treaty began with the participation of 25 Member States. The participating Countries have committed themselves to stepping up their efforts in the field of cyber defence, as well. Since 2017, 6 cyber-related PESCO projects have been launched:

1. European Secure Software Defined Radio (ESSOR)
2. Cyber Threats and Incident Response Information Sharing Platform

[26] European Commission: *Shaping Europe's Digital Future. Policy, European Cybersecurity Industrial, Technology and Research Competence Centre.* Brussels, 19 September 2018.

[27] European Commission: *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe.* Brussels, 6.5.2015, COM(2015) 192 final.

[28] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA.

3. Cyber Rapid Response Teams and Mutual Assistance in Cyber Security
4. Strategic Command and Control (C2) Systems for CSDP Missions and Operations
5. European High Atmosphere Airship Platform (EHAAP) – Persistent Intelligence, Surveillance and Reconnaissance (ISR) Capability
6. One Deployable Special Operations Forces (SOF) Tactical Command and Control (C2) Command Post (CP) for Small Joint Operations (SJO) – (SOCC) for SJO[29]

European Union Cyber Defence Policy Framework (2018)

In October 2018, the European Council called for measures able to respond to and deter cyberattacks and to build strong cybersecurity in the EU in order to strengthen its capacities. In view of the changing security challenges, the Council adopted a revised version of the EU Cyber Defence Policy Framework in October 2018. The updated version of the framework identified priority areas for cyber defence and clarified the roles of actors.

Scope and Objectives

> "To respond to changing security challenges, the EU and its Member States have to strengthen cyber resilience and to develop robust cyber security and defence capabilities. The EU Cyber Defence Policy Framework (CDPF) supports the development of cyber defence capabilities of EU Member States as well as the strengthening of the cyber protection of the EU security and defence infrastructure, without prejudice to national legislation of Member States and EU legislation, including, when it is defined, the scope of cyber defence.
> Cyberspace is the fifth domain of operations, alongside the domains of land, sea, air, and space: the successful implementation of EU missions and operations is increasingly dependent on uninterrupted access to a secure cyberspace, and thus requires robust and resilient cyber operational capabilities.
> The objective of the updated CDPF is to further develop EU cyber defence policy by taking into account relevant developments in other relevant fora and policy areas and the implementation of the CDPF since 2014. The CDPF identifies priority areas for cyber defence and clarifies the roles of the different European actors, whilst fully respecting the responsibilities and competences of Union actors and the Member States as well as the institutional framework of the EU and its decision-making autonomy."[30]

[29] EU Cyber Direct: *Cyber-related PESCO Projects.* Brussels, 12 November 2019; Council of the European Union: *Permanent Structured Cooperation (PESCO)'s Projects – Overview.* 2019.

[30] Council of the European Union: *EU Cyber Defence Policy Framework, (as updated in 2018).* Brussels, 19 November 2018(OR. en).

The document refers to the implementation of the goals and priorities set in the 2016 Global Strategy and the Joint Declaration on EU–NATO Cooperation. However, it emphasised that a number of other EU policies also contribute to achieving the objectives of cyber defence policy. This policy framework also takes into account regulations in civil areas (e.g. the Network and Information Security Directive) in order to contribute to the EU's strategic autonomy also in the area of cyberspace.

The policy framework highlights that, in accordance with the Council Conclusions on Cybersecurity of November 2017, there are growing linkages between the areas of cybersecurity and defence, and that there is a need to encourage cooperation between civilian and military incident response communities. The Council document emphasised that in a particularly serious cyber incident or crisis, the Solidarity Clause and/or the Mutual Assistance Clause of the Lisbon Treaty could also be activated.[31]

The policy framework identifies six priority areas: (1) developing cyber defence capabilities; (2) protecting EU CSDP communication and information networks; (3) training and exercises; (4) research and technology; (5) civil–military cooperation; and (6) enhancing cooperation with international partners.[32]

The EU's Cybersecurity Strategy for the Digital Decade (2020)

In December 2020, the new EU's cybersecurity strategy was completed by the European Commission and the European External Action Service. The deep crises caused by the Covid-19 pandemic not only accelerated the process of digitalisation but also led to a higher level of awareness in the EU. The strategy aims to strengthen resilience to cyber threats and provide reliable and secure services and digital tools for all citizens and businesses. The document aims to enable citizens and businesses to acquire these benefits. The strategy underlines the crucial role of cybersecurity for a growing economy, democracy and society. The objective of this strategy is to reinforce user confidence in digital tools. The strategy emphasises three main areas of EU action: (1) resilience, technological sovereignty and leadership; (2) building operational capacity to prevent, deter and respond (to cyberattacks); and (3) advancing a global and open cyberspace through increased cooperation.[33]

[31] Ibid. 6.

[32] Ibid. 8.

[33] European Commission: *Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade.* Brussels, 16.12.2020 JOIN(2020) 18 final.

In March 2021, the Council adopted conclusions on the cybersecurity strategy, highlighting that cybersecurity is an essential tool for building a resilient, green and digital Europe. The Council sets as a key objective of realising strategic autonomy at the same time as preserving an open economy. The conclusions aim at enabling the EU to make autonomous choices in the field of cybersecurity and to achieve the EU's digital leadership and strategic capacities.[34]

Digital Europe Programme (DIGITAL) (2021–2027)

The Digital Europe Programme (DIGITAL) is a part of the current long-term EU budget, the Multiannual Financial Framework 2021–2027. It is a new funding programme to bring digital technologies to businesses, citizens and public administrations. It provides strategic funding with a budget of €7.5 billion to support projects in five key capacity areas: (1) in supercomputing; (2) artificial intelligence; (3) cybersecurity; (4) advanced digital skills; and (5) ensuring a wide use of digital technologies across the economy and society, including through Digital Innovation Hubs. The new EU funding program aims to speed up the economic recovery and shape the digital transformation of Europe's society and economy, providing benefits to a wide range of stakeholders, but especially to small and medium-sized enterprises.[35]

The Institutional Framework Regarding the Cybersecurity of the EU

Due to the comprehensive nature of this issue, practically all institutions, bodies and agencies in the European Union are involved in the preparation and implementation of cybersecurity policy.

[34] Council of the European Union: *Draft Council Conclusions on the EU's Cybersecurity Strategy for the Digital Decade.* Brussels, 9 March 2021(OR. en).

[35] European Commission: *The Digital Europe Programme.* s. a.; Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 Establishing the Digital Europe Programme and Repealing Decision (EU) 2015/2240 (Text with EEA Relevance).

Table 2. *Cybersecurity in the EU: Areas of responsibility and institutional framework*

Cybersecurity			
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			
	EU-LISA	ESDC	
ECCC			EDA
			GSA

Source: Compiled by the author based on Bendiek (2018): op. cit. 4.

European Commission

The European Commission intends to strengthen cybersecurity capabilities. It also initiates and promotes policy-making and legislative processes in this field. The main Directorates-General (DG) responsible for areas related to cybersecurity are DG Connect (Communications Networks, Content and Technology) and DG Migration and Home (cybercrime). The main tasks of the Directorate-General Connect are linked to developing a digital single market and promoting policy-making processes related to cybersecurity. The Directorate-General Migration and Home is responsible for initiating and developing cybercrime policy. The Directorate-General for Informatics (DG Digit) provides digital services for departments of the European Commission and other EU institutions. Digit hosts CERT-EU (Computer Emergency Response Team).[36] DG Human Resources and Security is responsible for the Commission's staff, information and assets. It also provides investigations regarding incidents that covers counter-intelligence and counter-terrorism activities as well.[37]

[36] European Court of Auditors (2019): op. cit. 31.

[37] European Commission: *Departments and Executive Agencies.* s. a.

Computer Emergency Response Team (CERT-EU)

In the Digital Agenda for Europe adopted in 2010, the European Commission decided to establish a Computer Emergency Response Team for the EU institutions (CERT-EU) supporting all Union institutions, bodies and agencies. According to the Agenda, these CERTs had to be set up not only at EU level but also at Member State level in order to have a network of national and governmental CERTs in place by 2012. The CERT-EU was established in 2011 and it is hosted by the European Commission. Following a one-year pilot phase, the CERTs have been operating at full capacity since September 2012. The CERT-EU is composed of IT security experts from the main EU Institutions, and it cooperates with other CERTs in the Members States and with specialised IT security companies. The task of the newly set up permanent groups is to help them to respond to incidents, particularly those affecting information security. CERT-EU prepares reports and briefings on cyber threats concerning EU institutions, bodies and agencies. It provides an information-sharing platform. In 2018, CERT-EU finalised a non-binding memorandum of understanding with ENISA, EC3 and the European Defence Agency in order to increase cooperation and coordination with those agencies. It also signed a technical agreement with NATO's computer incident response capability (NCIRC).[38]

The role of CERTs is to prevent weaknesses in network security, to identify threats and to address vulnerabilities. In order to maintain and restore system security, the groups warn their clients about existing security vulnerabilities and threats, propose measures to reduce the risks.

European Network and Information Security Agency (ENISA)

The European Network and Information Security Agency (ENISA) was established in 2004. The agency, which has a mainly advisory role, has been operating in Athens and has had a second office in Heraklion since 2005. From 2005, the Agency's role was to

[38] European Court of Auditors (2019): op. cit. 6.

> "contribute to securing Europe's information society by raising awareness of network and information security and to develop and promote a culture of network and information security in society for the benefit of citizens, consumers, enterprises and public sector organizations in the Union."[39]

In parallel with the development of the first cybersecurity strategy, a new Regulation of the European Parliament and of the Council on the operation of ENISA was adopted on 21 May 2013, extending the Agency's mandate until 2020 and strengthening its capacity to tackle cyberattacks and other information security challenges.[40]

The first EU legislation on cybersecurity, the 2016 NIS Directive gave a central role to the ENISA in supporting the implementation of the Directive. The Agency provides the secretariat for the Network Security Response Teams (CSIRTs) and actively supports cooperation between CSIRTs.

Since 2019, following the new legislation of the Cybersecurity Act (Regulation 2019/881), ENISA has been tasked to support Member States, EU institutions and all other stakeholders in their cyber policies, and to prepare the 'European cybersecurity certification schemes' that serve as the basis for certification of ICT products, processes and services that support the proper delivery of the Digital Single Market. ENISA will play a central role in the development of certification schemes.

The Agency's new tasks will include:

- organising pan-European Cybersecurity Exercises
- the development and evaluation of National Cybersecurity Strategies
- CSIRTs cooperation and capacity building
- studies on IoT and smart infrastructures, addressing data protection issues, privacy enhancing technologies and privacy on emerging technologies, eIDs and trust services, identifying the cyber threat landscape, and others
- supporting the development and implementation of the European Union's policy and law on matters relating to network and information security (NIS)
- assisting Member States and European Union institutions, bodies and agencies in establishing and implementing vulnerability disclosure policies on a voluntary basis[41]

[39] Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA), Article 1(1).

[40] Regulation (EU) No 526/2013.

[41] ENISA: *About ENISA – The European Union Agency for Cybersecurity.* s. a.

The exercises organised by ENISA have helped to prepare national authorities to strengthen preparedness and resilience to cyber threats.

Computer Security Incident Response Team (CSIRTs)

The transposition of the 2016 Directive of the European Parliament and of the Council on the security of network and information systems (2016/1148) at Member State level necessitated the establishment of a network of Computer Security Incident Response Teams, i.e. CSIRTs. The EU-wide network is composed of CSIRTs in the Member States and representatives of the Network Security Emergency Response Teams (CERT-EU). The European Commission takes part in the network as an observer. ENISA supports the cooperation between CSIRTs appointed by the EU Member States, and it provides the secretariat. The CSIRTs Network offers a forum to exchange information and build trust.[42]

European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC)

In April 2021, the Council reinforced the selection of Bucharest as the seat of the new European Cybersecurity Industrial, Technology and Research Competence Centre (Cybersecurity Competence Centre, ECCC), which will improve the coordination of research and innovation in cybersecurity. It will also bring together the main European stakeholders, and it will help to promote pooling investment in cybersecurity research, technology and industrial development. The new centre will closely cooperate with ENISA.[43]

In May 2021, the European Parliament and the Council adopted the regulation establishing the ECCC and the Network of National Coordination Centres (Cyber NCCs).[44] Although the ECCC is not a formal EU agency, but

[42] ENISA: *CSIRTs Network*. s. a.

[43] Council of the European Union: *Draft Council Conclusions on the EU's Cybersecurity Strategy for the Digital Decade.* Brussels, 9 March 2021(OR. en).

[44] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 Establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

> "it will pool resources from the EU, Member States and industry to improve and strengthen technological and industrial cybersecurity capacities, enhancing the EU's strategic autonomy in the field of cybersecurity. It will offer a possibility to consolidate part of the cybersecurity-related activities funded under Horizon Europe, the Digital Europe Programme and the Recovery and Resilience Facility – funding streams totalling up to EUR 4.5 billion over the next six years."[45]

The aim of this process is to create an EU Cyber Shield composed of a network of Security Operations Centres by 2023, in order to detect cyberattacks early enough to enable proactive actions. In the future, it may be able to use Artificial Intelligence-powered technologies. Numerous Member States have planned the development of such national centres in the framework of their Recovery and Resilience plans. The European Commission allocates funds from the Digital Europe Programme to support their efforts.[46]

Europol EC3

In 2013, the European Cybercrime Centre (EC3) was set up at the headquarters of Europol in The Hague. The aim of the new centre was to protect European citizens and businesses from cyber threats and help governments against cybercrime. From the outset, the new EU headquarters focused on illegal online activities by organised criminal groups, in particular attacks on electronic banking and other financial activities. The centre provides support for more effective protection of social networking profiles against cybercrime and information and analysis to national law enforcement authorities. Since its inception, the EC3 publishes yearly the Internet Organised Crime Threat Assessment (IOCTA). EC3 has made a significant contribution to the fight against cybercrime by participating in a number of outstanding operations and providing operational support on the ground.[47]

[45] European Commission: *Joint Communication to the European Parliament and the Council. Report on Implementation of the EU's Cybersecurity Strategy for the Digital Decade.* Brussels, 23.6.2021 JOIN(2021) 14 final. 2.

[46] Ibid.

[47] Europol: *European Cybercrime Centre – EC3.* s. a.

Eurojust

According to the Lisbon Treaty, the Eurojust is responsible for supporting and strengthening the coordination and cooperation between national investigating and prosecuting authorities in relation to serious crimes affecting two or more Member States (Article 85). The European Union Agency for Criminal Justice Cooperation (Eurojust) is the successor to the Judicial Cooperation Unit of the European Union created in 2002. The new regulation of Eurojust was adopted in 2018.[48]

The European Judicial Cybercrime Network (EJCN) was established in 2016 to promote "contacts between practitioners specialised in countering the challenges posed by cybercrime, cyber-enabled crime and investigations in cyberspace, and to increase efficiency of investigations and prosecutions". [49]

European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA)

The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA), was established in 2011 (Establishing Regulation (EU) No 1077/2011) and started its activities in 2012. The headquarters of this agency are in Tallinn, Estonia, and its operational centre is in Strasbourg, France. A business continuity site for the systems under management is situated in Sankt Johann im Pongau, Austria and a Liaison Office in Brussels, Belgium.

The EU-Lisa is responsible for the operational management of large-scale IT systems, which are essential instruments in the implementation of the Union's policies in the area of justice, security and freedom. It facilitates the implementation of the asylum, border management and migration policies of the EU.

The Agency is currently providing operational management of the Eurodac (a large-scale fingerprint database mainly for asylum applications), the SIS II (the second generation Schengen Information System) and the VIS (Visa Information System).[50]

[48] Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and Replacing and Repealing Council Decision 2002/187/JHA.

[49] Eurojust: *European Judicial Cybercrime Network.* s. a.

[50] EU-LISA: *EU-LISA. Who We Are.* s. a.

European External Action Service (EEAS)

The European External Action Service manages the diplomatic relations of the European Union conducting CFSP. The EEAS has a central role in the field of cyber diplomacy, strategic communication and the policies concerning cyber defence. This body hosts intelligence and analysis centres dealing with cyber issues as well for civilian and military situational awareness (the Single Intelligence Capability: European Union Intelligence Analysis Centre (INTCEN) and the Military Staff Intelligence Directorate). The Hybrid Fusion Cell was established in 2016 within the EU Intelligence Analysis Centre to improve situational awareness and support decision-making. It gathers and analyses classified and open source information concerning hybrid threats.[51]

European Defence Agency (EDA)

The European Defence Agency was established in 2004 as an intergovernmental agency of the Council of the European Union. The EDA supports the Member States and the Council in their effort to improve defence capabilities through European cooperation. According to the Council conclusion, the EDA aims to develop cyber defence capabilities related to CSDP, to civil–military cooperation and synergies, to raise awareness and to cooperate with relevant international partners.[52]

The EU Approach to Cyber Diplomacy

The EU has started to play an increasingly active role not only in deepening the integration process between its own Member States, but also in resolving international disputes related to cybersecurity and cyber defence.[53] The 2013 strategy set out the EU's international cyber policy. In addition to protecting a free and open Internet, the new policy aimed to promote international law of

[51] European Court of Auditors (2019): op. cit. 50.
[52] Rehrl (2018): op. cit. 93–94.
[53] Thomas Renard: EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain. *European Politics and Society,* 19, no. 3 (2018). 321–337.

responsible state behaviour and confidence-building measures in cyberspace and to improve cooperation with the EU's strategic partners. To this end, negotiations have begun with the United States, China, Japan, South Korea, India and Brazil. During the negotiations, the parties discussed, inter alia, the areas of international security in cyberspace, resilience, cybercrime, Internet governance and cybersecurity standards. An important milestone in 2015 was the adoption of Council conclusions on cyber diplomacy to support the EU's collective efforts.[54]

- EU approach to cyber diplomacy at global level
- promotes and protects human rights and is grounded on the fundamental EU values of democracy, human rights and the rule of law, including the right to freedom of expression, access to information and right to privacy
- ensures that the Internet is not abused to fuel hatred and violence and safeguards that the Internet remains, in scrupulous observance of fundamental freedoms, a forum for free expression in full respect of law
- promotes a cyber policy informed by gender equality
- advances European growth, prosperity and competitiveness and protects EU core values, inter alia, by strengthening cybersecurity and improving cooperation in fighting cybercrime
- contributes to the mitigation of cybersecurity threats, conflict prevention and greater stability in international relations through the use of diplomatic and legal instruments
- promotes the efforts to strengthen the multi-stakeholder model of Internet governance
- fosters open and prosperous societies through cyber capacity building measures in third countries that enhances the promotion and protection of the right to freedom of expression and access to information and that enables citizens to fully enjoy the social, cultural and economic benefits of cyberspace, including by promoting more secure digital infrastructures
- promotes the sharing of responsibilities among relevant stakeholders, including through cooperation between the public and private sectors as well as research and academic institutions on cyber issues[55]

[54] Rehrl (2018): op. cit. 23.

[55] Council of the European Union: *Council Conclusions on Cyber Diplomacy.* Brussels, 11 February 2015 (OR. en).

According to Bendiek "it is a politically and legally controversial issue whether attacked states should adopt offensive countermeasures, such as hack-backs, to neutralise the source of a cyber-attack, […] and the state requires military and strategic cyber weapons as well as a legal basis for their deployment in order to respond to cyberattacks."[56]

At the international level, the EU attached importance to the strict application of international law, in particular the UN Charter and international humanitarian law, and the full implementation of universal non-binding cyber norms, rules and principles of responsible state behaviour in cyberspace for conflict prevention and stability. The EU also promotes the development of confidence building measures and cooperation with other international organisations. According to Rehrl, the OSCE, which is a very important partner of the EU, is the most advanced organisation in the field of confidence-building measures at the regional level.[57]

Due to the growing level of cyber threats and challenges in recent years, cyber diplomacy has become an integral part of Common Foreign and Security Policy. EU Member States agreed on strengthening cyber diplomacy capabilities within the European External Action Service in 2015. The implementation plan on security and defence confirmed this intention in 2016. Important bodies (EU INTCEN and EUMS INT) started to deal with cyber issues.[58]

In 2017, the Council of the European Union agreed to develop a framework for joint EU diplomatic action against malicious cyber activities by state and non-state actors. The so-called Cyber Diplomacy Toolbox was built on the EU's CFSP Policy Toolbox. The EU stands ready to take action on Common Foreign and Security Policy measures, including restrictive measures against activities using information and communication technologies (ICT) that could exhaust the notion of an act of violation of international law.[59]

In line with the EU's cyber diplomatic approach, the joint action will contribute to conflict prevention, the reduction of cybersecurity threats and the enhancement of stability in international relations. The Council set the goal of providing a framework for joint EU diplomatic action to facilitate cooperation,

[56] Annegret Bendiek: The EU as a Force for Peace in International Cyber Diplomacy. *SWP Comment,* no. 19 April 2018. 1–2.

[57] Rehrl (2018): op. cit. 25.

[58] Bendiek (2018): op. cit. 1–2.

[59] Council of the European Union: *Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").* Brussels, General Secretariat of the Council, 2017a.

promote risk reduction and influence the behaviour of potential attackers. This EU diplomatic response will make full application of measures used under the Common Foreign and Security Policy, including restrictive measures and possible 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".[60]

On 11 October 2017, the Political and Security Committee adopted implementing guidelines for the Cyber Diplomacy Toolbox. The document listed five categories of measures within the cyber diplomacy toolkit. These included restrictive measures and the procedure for imposing such measures.[61]

According to the 2018 Cyber Defence Policy Framework, the events of previous years have further highlighted the need for more cooperation within the international community in order to prevent conflicts and strengthen the stability of cyberspace.

> "The EU is promoting, in close cooperation with other international organisations, in particular the UN, the OSCE and the ASEAN Regional Forum, a strategic framework for conflict prevention, cooperation and stability in cyberspace, which includes (i) the application of international law, and in particular the UN Charter in its entirety, in cyberspace; (ii) the respect of universal non-binding norms, rules and principles of responsible State behaviour; (iii) the development and implementation of regional confidence building measures (CBMs). The Cyber Defence Policy Framework should also support this endeavour."[62]

In 2019, the EU made significant progress in making the Cyber Diplomacy Toolbox against malicious cyber activities operational and effective. In order to achieve the objectives laid down in its conclusions of June 2018 and October 2018, the European Council decided to introduce EU restrictive measures to help improve the response and deterrence capacity of the Union. On 17 May 2019, a Council Decision [(CFSP) 2019/797] and a Council Regulation [(EU) 2019/796] was taken on restrictive measures against cyberattacks threatening the Union or its Member States.[63] The decision identifies the applicability of measures within the CFSP, if necessary, restrictive measures against malicious cyber activities, and the regulation allows

[60] Council of the European Union: Cyber Attacks: EU Ready to Respond with a Range of Measures, Including Sanctions. *Press Release,* 19 June 2017b.

[61] Council Decision (CFSP) 2019/797 of 17 May 2019, Concerning Restrictive Measures against Cyber-attacks Threatening the Union or its Member States.

[62] Council of the European Union (2018): op. cit. 8.

[63] Council Decision (CFSP) 2019/797.

the EU to impose sanctions as a response to cyberattacks with a significant effect which constitute an external threat to the Union or its Member States.[64]

The new legal framework has thus made it possible for the EU to impose sanctions (e.g. asset freeze, travel ban) to deter and respond to cyberattacks that constitute an external threat to the Union or its Member States. Those sanctions should be effective, proportionate and dissuasive.[65]

In June and October 2020, the Council added several natural and legal persons or entities to the list of natural and legal persons, entities and bodies subject to restrictive measures in accordance with Council Decision (CFSP) 2019/797 in order to prevent, discourage, deter and respond malicious behaviour in cyberspace. The natural or legal persons, entities or bodies named in the Decision are responsible for, providing or supporting cyberattacks, including attempted cyberattacks against the OPCW, cyberattacks known as "WannaCry" and "NotPetya", Operation Cloud Hopper, and the cyberattack on the Federal Parliament of Germany in April and May 2015.[66]

Conclusions

EU decision-makers initially considered the field of digitisation and the use of ICT tools primarily as economic issues. However, the process of securing this area began in early 2010, with the 2013 cybersecurity strategy as a milestone.

In recent years, EU Member States and institutions have continued to be the main targets of cyberattacks and disinformation campaigns. Just a few months after the adoption of measures to sanction serious attacks on the Union and its Member States, a cyberattack on the Bulgarian tax authorities in 2019 resulted in the theft of data from 5 million citizens. In early 2019, the Spanish and Lithuanian Ministries of Defence, as well as the Finnish Ministry of Justice, also fell victim to cyberattacks. In addition to the unprecedented global health crisis, the 2020 coronavirus epidemic has also contributed to the spread and growth of various types of cyberattacks.[67]

[64] Ibid.

[65] European Commission: *Report on the Implementation of the Action Plan Against Disinformation. Joint Communication to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions.* Brussels, 14.6.2019 JOIN(2019) 12 final. 8.

[66] Council Decision (CFSP) 2020/1127; Council Decision (CFSP) 2020/1537.

[67] Daniel Fiott – Vassilis Theodosopoulos: *Yearbook of European Security.* EUISS, 2020.

References

Bendiek, Annegret: *The EU as a Force for Peace in International Cyber Diplomacy. SWP Comment,* no. 19 April 2018. Online: www.swp-berlin.org/fileadmin/contents/products/comments/2018C19_bdk.pdf

Council Decision (CFSP) 2019/797 of 17 May 2019, Concerning Restrictive Measures against Cyber-attacks Threatening the Union or its Member States. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019D0797&from=EN

Council Decision (CFSP) 2020/1127 of 30 July 2020, Amending Decision (CFSP) 2019/797 Concerning Restrictive Measures against Cyber-attacks Threatening the Union or its Member States. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=HU

Council Decision (CFSP) 2020/1537 of 22 October 2020 Amending Decision (CFSP) 2019/797 Concerning Restrictive Measures against Cyber-attacks Threatening the Union or its Member States. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1537&from=EN

Council of the European Union: *Report on the Implementation of the European Security Strategy. Providing Security in a Changing World.* Brussels, 11 December 2008. Online: www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/reports/104630.pdf

Council of the European Union: *European Security Strategy. A Secure Europe in a Better World.* Brussels, General Secretariat of the Council, 2009. Online: https://doi.org/10.2860/1402

Council of the European Union: *Internal Security Strategy for the European Union. Towards a European Security Model.* Brussels, General Secretariat of the Council, 2010. Online: https://doi.org/10.2860/87810

Council of the European Union: *EU Cyber Defence Policy Framework.* Brussels, 18 November 2014. Online: www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf

Council of the European Union: *Council Conclusions on Cyber Diplomacy.* Brussels, 11 February 2015 (OR. en). Online: http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf

Council of the European Union: *Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").* Brussels, General Secretariat of the Council, 2017a. Online: http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

Council of the European Union: Cyber Attacks: EU Ready to Respond with a Range of Measures, Including Sanctions. *Press Release,* 19 June 2017b. Online: www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

Council of the European Union: *EU Cyber Defence Policy Framework, (as updated in 2018).* Brussels, 19 November 2018(OR. en). Online: http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf

Council of the European Union: *Permanent Structured Cooperation (PESCO)'s Projects – Overview.* 2019. Online: www.consilium.europa.eu/media/39762/pesco-overview-of-first-collaborative-of-projects-for-press.pdf

Council of the European Union: *Draft Council Conclusions on the EU's Cybersecurity Strategy for the Digital Decade.* Brussels, 9 March 2021(OR. en). Online: https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf

Council of the European Union: Bucharest-based Cybersecurity Competence Centre Gets Green Light from Council. *Press Release,* 20 April 2021. Online: www.consilium.europa.eu/en/press/press-releases/2021/04/20/bucharest-based-cybersecurity-competence-centre-gets-green-light-from-council/

Council Regulation (EU) 2019/796 of 17 May 2019, Concerning Restrictive Measures against Cyber-attacks Threatening the Union or its Member States. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0796&from=EN

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

ENISA: *About ENISA – The European Union Agency for Cybersecurity.* s. a. Online: www.enisa.europa.eu/about-enisa

ENISA: *CSIRTs Network.* s. a. Online: www.enisa.europa.eu/topics/csirts-in-europe/csirts-network

EU Cyber Direct: *Cyber-related PESCO Projects.* Brussels, 12 November 2019. Online: https://eucyberdirect.eu/content_knowledge_hu/cyber-related-pesco-projects/

EU-LISA: *EU-LISA. Who We Are.* s. a. Online: www.eulisa.europa.eu/About-Us/Who-We-Are

Eurojust: *European Judicial Cybercrime Network.* s. a. Online: www.eurojust.europa.eu/Practitioners/Pages/EJCN.aspx

European Commission: Brussels, 1.6.2005, COM(2005) 229 final, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions "i2010 – A European Information Society for growth and employment". Commission of the European Communities, 2005. Online: lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:EN:PDF

European Commission: *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* JOIN/2013/01 final. Online: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/join_2013_1_en.pdf

European Commission: *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe.* Brussels, 6.5.2015, COM(2015) 192 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192

European Commission: *Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU.* Brussels, 13.9.2017, JOIN(2017) 450 final. Online: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX-%3A52017JC0450

European Commission: *State of the Union 2017 – Cybersecurity: Commission Scales Up EU's Response to Cyber-attacks.* Brussels, 19 September 2017. Online: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3193

European Commission: *Shaping Europe's Digital Future. Policy, European Cybersecurity Industrial, Technology and Research Competence Centre.* Brussels, 19 September 2018. Online:

https://ec.europa.eu/digital-single-market/en/european-cybersecurity-industrial-technology-and-research-competence-centre
European Commission: *Report on the Implementation of the Action Plan Against Disinformation. Joint Communication to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions.* Brussels, 14.6.2019 JOIN(2019) 12 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019JC0012&from=EN
European Commission: *Shaping the Digital Single Market.* 2020. Online: https://ec.europa.eu/digital-single-market/en/europe-2020-strategy
European Commission: *Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade.* Brussels, 16.12.2020 JOIN(2020) 18 final. Online: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0
European Commission: *Joint Communication to the European Parliament and the Council. Report on Implementation of the EU's Cybersecurity Strategy for the Digital Decade.* Brussels, 23.6.2021 JOIN(2021) 14 final. Online: https://digital-strategy.ec.europa.eu/en/library/first-implementation-report-eu-cybersecurity-strategy
European Commission: *The Digital Europe Programme.* s. a. Online: https://digital-strategy.ec.europa.eu/en/activities/digital-programme
European Commission: *Departments and Executive Agencies.* s. a. Online: https://ec.europa.eu/info/departments
European Council: *European Council Conclusions 19/21 December 2013.* Online: www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/ec/140245.pdf
European Court of Auditors: Challenges to Effective EU Cybersecurity Policy. *Briefing Paper,* March 2019. Online: www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf
European External Action Service: *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy.* 2016. Online: http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf
Europol: *European Cybercrime Centre – EC3.* s. a. Online: www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
Fiott, Daniel – Vassilis Theodosopoulos: *Yearbook of European Security.* EUISS, 2020. Online: www.iss.europa.eu/sites/default/files/EUISSFiles/YES_2020.pdf
Kovács, László: *Kiberbiztonság és stratégia.* Budapest, Dialóg Campus, 2018.
Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and Replacing and Repealing Council Decision 2002/187/JHA. Online: www.eurojust.europa.eu/hu/document/regulation-eu-20181727-14-november-2018-european-union-agency-criminal-justice-cooperation
Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA, (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA Relevance) PE/86/2018/REV/1. Online: https://eur-lex.europa.eu/eli/reg/2019/881/oj

Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA), Article 1(1). Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013R0526

Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 Establishing the Digital Europe Programme and Repealing Decision (EU) 2015/2240 (Text with EEA Relevance). Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-%3A32021R0694

Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 Establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. Online: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32021R0887

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

Renard, Thomas: EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain. *European Politics and Society,* 19, no. 3 (2018). 321–337. Online: https://doi.org/10.1080/23745118.2018.1430720

Dóra Molnár

European Cyber Diplomacy Landscape – France, the United Kingdom and Germany

Introduction

When it comes to cybersecurity, the saying "as many states, so many approaches" is certainly true. This is true not only globally, but also for European states. States have recognised the growing importance of this area at different times and have described a different trajectory in both the development of their cybersecurity strategic culture and its implementation. Accordingly, the importance of cyber diplomacy varies from state to state, although it is an undoubted fact that most states now emphasise the strategic importance of cyber relations, the need for cooperation and the need to establish rules of conduct in cyberspace at the strategic level. However, the proposed solutions are very different. For example, one group of states considers it necessary to create a comprehensive cyber convention, while others strongly oppose it along arguments based on the characteristics of cyber weapons.[1] Most states in the Western world are pushing for a multi-stakeholder governance model of the Internet, while the developing world, led by China and supported by Russia, is in favour of a multilateral solution in every possible forum. However, in addition to the many different approaches, there are several commonalities in public policies. Most states seek to make the most of the opportunities offered by international fora and organisations, but they also seek to build the widest possible network of bilateral contacts. The fault lines between individual states are well delineated on the basis of whether they manage to bring a bilateral cyber agreement under the roof.

The study examines three European states. Today, the United Kingdom is the world's leading cyber state, so it is impossible to ignore the British cyber diplomatic solutions. However, when it comes to diplomacy, France comes to

[1] These include, for example, the unresolved nature of control issues and the difficulty of rapid technological change and adaptation. See Fahad Nabeel: International Cyber Regime: A Comparative Analysis of the US–China–Russia Approaches. *Stratagem,* 1, no. 2 (2018). 8–27.

https://doi.org/10.36250/01039_03

mind as the first European state, so I will also start my study by presenting French characteristics. The third state surveyed is Germany, due to the country's leading European position and the unique intertwining of the economy and cyber politics. Each of the states surveyed has been advocating the need to regulate cyberspace for years, most recently joining the Joint Declaration on Advancing Responsible State Behaviour in Cyberspace on 23 September 2019, along with a further 24 states.[2] The U.S.-initiated statement underlined the need for a concerted and coordinated cyber effort to protect citizens, among other things, from a series of cyberattacks – adding that the attacks are being carried out by Russia and other adversaries. It has also been declared that inappropriate cyberspace behaviour will have consequences. In the following, I present the international activities of the three states and/or the main actors of the network of bilateral contacts, based on the national cyber strategies.

France as a Cyber Diplomatic Power

Perhaps it is no exaggeration to say that France has been a stronghold of diplomacy for centuries, and that the French are great masters of the use of "soft" tools in politics. The country's strength is given by its global role, based on its extensive diplomatic network: it has an unparalleled membership in multilateral and international organisations, with the highest number of foreign cultural missions and the 5th largest donor state.[3] It is therefore not surprising that French politics prefers to use the tools of diplomacy in cyberspace effectively – so much so that it is at the forefront of this field at European level. This justifies me starting my study of European countries with France, even if there is another European state in terms of cyber power potential that is ahead of the country.

The need for international cooperation in cyberspace as one of the necessary areas for action is already reflected in the first cyber strategy, *Protection and Security of Information Systems: A Strategy for France,* published in 2011.[4] This is specified in Senate Information Report No. 681, adopted in 2012, by

[2] U.S. Department of State: *Joint Statement on Advancing Responsible State Behavior in Cyberspace.* 23 September 2019.

[3] Consulat Général de France á Ekaterinbourg: *La diplomatie française à l'ère numérique.* 29 May 2019.

[4] Agence nationale de la sécurité des systèmes d'information: *Défense et sécurité des systèmes d'information. Stratégie de la France.* 2011.

emphasising the importance of bilateral relations as one of the ten priorities, and calling for joint action with the Organization for North Atlantic Cooperation (NATO) and the European Union (EU), dialogue with China and Russia, and supports the adoption of international confidence-building measures.[5] The 2013 White Paper emphasises the need for a "global governmental approach" to combat cyberattacks, in which France builds on its diplomatic, legal and political instruments.[6]

The country's cyber strategy was released in 2015 under the title *National Digital Security Strategy*.[7] The strategy sets out five main objectives, the fifth of which is entitled *Europe, Digital Strategic Autonomy, Cyberspace Stability.* France intends to participate in Europe's digital transformation through its allied relations, in three main ways: by setting out a roadmap for a European strategy with other EU volunteers, by strengthening the French presence and influence in international cyber talks, and by supporting other states in building cyber capabilities, thereby contributing to the global stability of cyberspace. According to the strategy, the main venues for increasing influence among the international organisations are the United Nations (hereinafter: the UN) and the Organization for Security and Cooperation in Europe (hereinafter: the OSCE), active participation in bilateral relations in the framework of diplomatic dialogue at ministerial level and in informal international fora with political decision-makers and academia. The area of cyber diplomacy was centralised to implement the strategy, and in 2015 the position of ambassador for cyber diplomacy and the digital economy was set up in the Ministry of Foreign Affairs.[8]

Since the adoption of the 2015 strategy, the international environment has changed significantly. It is enough to think of the series of cyberattacks following the terrorist attack on Charlie Hebdo or against the television channel TV5. The events also shed new light on the issue of cybersecurity in France and encouraged the country to take more active and vigorous national and international action.

The new approach is reflected in the Offensive Cyber Operations Doctrine, published on 18 January 2018, about three weeks before the release of the Cyber

[5] Sénat: *Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur la cyberdéfense.* Par le Sénateur M. Jean-Marie Bockel. Sénat session extraordinaire de 2011–2012. Enregistré á la Présidence du Sénat le 18 juillet 2012.

[6] Ministère des Armées: *Livre Blanc. Défense et sécurité nationale 2013.* Paris.

[7] SGDSN: *La stratégie nationale pour la sécurité du numérique.* 2015.

[8] The position, which has been called Digital Ambassador since 22 November 2017, was filled by David Martinon.

Defence Strategic Review. In the document, France openly states that cyber capabilities are part of its military activities and are ready to be deployed if necessary. This certainly marks a turning point in French cyber politics, which has so far been characterised by discreet diplomatic actions: even in case of blatant cyber conflicts such as the Russian-sponsored cyberattack on the Navy to find out about oil supply channels, France did not use offensive rhetoric, but sought to defuse tensions by using the means of dialogue.[9]

On 8 February 2018, the latest Cyber Defence Document entitled *Cyber Defence Strategic Review* was issued as the official material summarising the country's cyber defence ambitions.[10] Also known as the *White Paper on Cyber Defence,* the document sets out in several chapters the need for some cyber diplomatic action and sets out France's position on the issue. There is a separate chapter on international negotiations on the regulation of cyberspace, highlighting the role of the UN and the Group of Governmental Experts (GGE) and their achievements since 2013. At the 2016–2017 session, France put forward a separate proposal for a deeper regulation of the non-refoulement ban, which, although supported by the participating states, was stalled due to differing views on how to apply international law. Another chapter shows how the country performs internationally in cyberspace. It promotes dialogue and cooperation with its allies in order to prevent cyber conflicts, urges the regulation of cyberspace and aims to ensure European security and autonomy in cyberspace as well. From among its bilateral relationships it highlights its cyber relations with the United States,[11] China, India,[12] Brazil and Japan, adding that it will continue to cultivate deep ties with its Western allies, but will place increasing emphasis on the sub-Saharan region, where it urges the establishment of relations with the Francophone states. European cyber relations need to be organised along three issues: technical, regulatory and capacity issues, which require the formulation

[9] Arthur P. B. Laudrain: France's New Offensive Cyber Doctrine. *Lawfare,* 26 February 2019.

[10] SGDSN: *Revue stratégique de cyberdéfense.* 12 February 2018.

[11] The third stop of the Franco–American cyber dialogue was held on 22 January 2020 in Paris. The central topic of the meeting was the applicability of international law to cyberspace. Ministère de l'Europe et des Affaires Étrangères: *Troisième dialogue stratégique France*–États-*Unis en matière de cybersécurité (Paris, 22 janvier 2020).*

[12] The India–France Bilateral Cyber Dialogue was held for the third time on 20 June 2019, discussing primarily issues related to cyber norms. The importance of bilateral cyber relations is well signalled by India's invitation to the 2019 G7 summit from France, which held the presidency in 2019. Ministère de l'Europe et des Affaires Étrangères: *Indo–French Bilateral Cyber Dialogue (Paris, 20 June 2019).*

and adoption of common ground. The Franco–German system of relations occupies a prominent place in both bilateral and European relations. Cooperation between the two countries is very intensive and extensive, as evidenced by the two joint reports published so far.[13] Finally, the document calls for the adoption of an action doctrine that sets out fundamental issues such as the classification system for cyberattacks and the range of responses to cyber incidents. A global system for regulating cyberspace can only be implemented along the lines of principles such as prevention, cooperation and stability.

Despite a more "offensive" attitude, diplomatic moves will certainly continue to play a key role in French politics in the future. It is no coincidence that France is one of the most active Member States in various international organisations when it comes to cybersecurity issues. Not only in the UN, as discussed above in relation to the GGE, but also in NATO, the G7 and the OSCE.[14] In the latter organisation, France played a very important role in the adoption of the two packages of confidence-building measures related to cybersecurity. With regard to the French participation in the G7, I would like to highlight the meeting held in the small French town of Dinard on 5–6 April 2019, where the so-called Dinard Declaration on the Initiation of Cyberspace Rules was accepted.[15] It welcomed the UN General Assembly's supportive approach to the applicability of international law in cyberspace and reaffirmed their intention to promote an open, secure, stable, accessible and peaceful cyberspace. At the same time, they reaffirmed their intention to formulate a Cyber Norm Initiative – CNI, which was finalised on 26 August 2019 with ten basic rules applicable in cyberspace.[16] All of this fits well with the success story of French soft politics, although it should be added that there was no precedent for the adoption of such an initiative. From 12 to 14 November 2018, the UNESCO Headquarters in Paris hosted the thirteenth annual meeting of the Internet Governance Forum, where French President Emmanuel Macron himself announced the Paris Call for Confidence

[13] Agence nationale de la sécurité des systèmes d'information: *ANSSI/BSI Common Situational Picture.* Vol. 1 – July 2018; Agence nationale de la sécurité des systèmes d'information: *Second Edition of the Franco–German Common Situational Picture.* 21 May 2019.

[14] Ministère de l'Europe et des Affaires Étrangères: *La France et la cybersécurité.* s. a.

[15] Ministère de l'Europe et des Affaires *Étrangères*: *Dinard Declaration on the Cyber Norm Initiative.* 06 April 2019.

[16] Ministère de l'Europe et des Affaires *Étrangères*: *Inititative pour des normes dans le cyberespace. Synthese des enseignements tirés et des bonnes pratiques.* 26 August 2019.

and Security in Cyberspace.[17] The widespread acceptance of the call is well indicated by the fact that it was immediately supported by more than 500 entities (state, organisation and company).[18] However, the completeness of the picture also includes the fact that each of the three "big" states rejected the initiative, torpedoing its global acceptability. With the call and a number of similar initiatives, France aims to see the country as a cyber power worldwide. Perhaps this goal also guided the country on 9 September 2019, when the French Ministry of Defence set out in an official document its views on how international law, according to France, could be applied in cyberspace[19] – thereby also taking on a pioneering role in cyber diplomacy.

Germany

Although Germany has been actively involved in UN cybersecurity consultations and other bilateral and multilateral fora since 2004, cooperation has been limited to technical issues. Although the first German cybersecurity strategy in 2011 mentioned the international and diplomatic dimensions of cybersecurity, until the Snowden case, Germany did not play a significant role in cyberspace. Only after the case Germany together with Brazil, due to the involvement of German Chancellor Angela Merkel, initiated the adoption of a UN resolution on the protection and inviolability of the right to privacy in the digital age, which resulted in the adoption of UN General Assembly Resolution No. 68/167 on 18 December 2013. This was a major cyber diplomatic success for Germany, especially because it managed to raise this issue to global level with South American support. From then on, Germany has become an active supporter of cyber diplomacy. In 2016, under the German chairmanship of the OSCE, the second package of confidence-building measures in cyberspace was adopted, and in 2016–2017, German diplomatic representatives also chaired the UN GGE.

[17] Ministère de l'Europe et des Affaires Étrangères: *Appel de Paris pour la confiance et la sécurité dans le cyberespace.* 12 November 2018.

[18] Ministère de l'Europe et des Affaires Étrangères: *Cybersécurité: Appel de Paris du 12 novembre 2018 pour la confiance et la sécurité dans la cyberespace. Liste des soutiens à l'appel de Paris (actualisé le 14 novembre 2018).*

[19] Przemyslaw Rogusky: France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I. *Opinio Juris,* 24 September 2019.

The foundations for increasingly active German action must be found in the country's cybersecurity strategy. In 2016, the country's second cyber strategy was released[20] which already highlights the importance of cooperation, which, however, must not be limited to national frameworks, but must establish pan-European and even global channels of cooperation. The document identifies four areas for action, one of which is the appropriate positioning of Germany in European and international cybersecurity policy discussions. This clearly shows that cyber diplomacy has established itself as a priority area and has become a fundamental factor influencing the security of a country. As part of this, Germany also emphasises the importance of bilateral partnerships, especially in areas such as information sharing and the coordination of security issues related to cross-border services, capacity sharing and in the field of development cooperation, where security and confidence-building measures are the key to success.

Germany is also gradually putting the strategy into practice with bilateral relations playing an enhanced role. The *United States* is a key strategic partner, so it is no coincidence that their cyber dialogue also has a long and meaningful history. Since 2012, a bilateral cyber meeting has been held annually, one year in Washington, the other in Berlin. During the meetings, issues such as the applicability of international law in cyberspace or the online enforcement of human rights are discussed like in 2016, but their common thinking of the multi-stakeholder model of cyberspace is also well established.[21] A consensus was reached with *China* in November 2016 that the two states would continue the dialogue on cyber issues through a special mechanism, but no bilateral agreement has been signed to date.[22] Most recently, Chancellor Merkel held talks in China in January 2020 to create a German–Chinese cyber agreement (similar to the U.S.–China agreement), but its precondition is the introduction of a "no spy" clause due to the American Huawei scandal. However, when asked about the convention, the Chancellor only said diplomatically that Germany and China have been constantly discussing a number of bilateral and international issues with each

[20] Federal Ministry of the Interior: *Cyber-Sicherheitsstrategie für Deutschland 2016* [Cybersecurity Strategy for Germany 2016].

[21] U.S. Department of State: *Joint Statement on U.S.–Germany Cyber Bilateral Meeting.* 24 March 2016.

[22] Christopher Burgess: Dissecting China's Global Bilateral Cybersecurity Strategy. *Security Boulevard,* 09 October 2016.

other on several levels.[23] At the same time, the German bilateral palette is not limited to the large partner states, but presents an extremely colourful picture. Germany, for example, has good bilateral cyber relations with Singapore. In 2017, the Prime Minister of Singapore paid a visit to Germany, during which the two sides signed a joint memorandum of understanding on cybersecurity cooperation in areas such as information sharing or joint research. The visit was reciprocated by Chancellor Merkel in June 2018, and the leaders of the two countries also concluded a defence treaty with a separate cyber clause.[24]

Germany is active in discussing cybersecurity issues in a number of international institutions, but perhaps the role of the *OSCE* stands out among all these actions. At the same time, Germany was predestined to take the lead in OSCE initiatives. On the one hand, because historically they are linked by political and economic threads to both the East and the West, and the OSCE also connects the leading powers in these regions. On the other hand, because Germany is a leading state in this area – it is enough to think about the technical standards and regulations set up in the field of data protection. Thirdly, because Germany participates effectively in organisations (such as the GGE) that set standards and rules in cyberspace, furthermore it can also benefit from the experience it has gained here.[25]

In 2013, the OSCE developed the first package of confidence-building measures in cyberspace, which provided an appropriate basis for moving forward. During the 2016 German OSCE Chairmanship, the possible scope of confidence- and security-building measures was discussed separately in all three baskets. For the first basket, only a series of voluntary agreements on military cooperation between Member States were recorded in 2013. It was agreed that the OSCE would be used as a platform to exchange information on cyberattacks and to mutually support the expansion of national capabilities. The German presidency explicitly aimed to involve engineers (primarily IT professionals) in cyber diplomacy (not just concerning the first basket), which is expected to have the effect of reducing diplomatic tensions, such as the developments at the Pugwash conferences since the 1950s. The German Information Security Act,

[23] Guy Chazan: German Cyber Security Chief Backs 5G 'No Spy' Deal over Huawei. *Financial Times,* 28 February 2020.

[24] Prashanth Parameswaran: Singapore–Germany Cyber Cooperation in Focus with Introductory Visit. *The Diplomat,* 14 August 2018.

[25] German Institute for International and Security Affairs: *Three Priorities for Cyber Diplomacy under the German OSCE Chairmanship 2016.* Berlin, 11 November 2015.

adopted in 2015, which set higher security requirements for critical infrastructure protection, served as a reference point for the second steps in the economic basket. German law also served as a reference when the NIS Directive was drafted. The central German cyber body, the Federal Office for Information Security (BSI)[26] has served as a model of technical expertise for many OSCE partners.

All these developments open a new horizon in the context of OSCE economic cooperation. In the case of the third basket, the issue of human rights, including freedom of expression on the Internet, is problematic. Above all, the German Presidency had to find an answer to the dilemma of censorship, network surveillance and copyright issues.

Germany makes the regulation of cyberspace a top foreign policy priority. He strongly advocates that global issues can only be resolved through common regulation – and this includes cybersecurity. The problem cannot be tackled at national level alone, but requires close cooperation between states, international organisations, NGOs and academia. It declares the applicability of international law in cyberspace and supports the multilateral approach.[27] In any case, it should be considered a diplomatic success that in November 2019, Germany was able to give home to the UN Internet Governance Forum.

The Leading (European) Cyber Power: The United Kingdom

The U.K., like the great powers, recognised the importance of cybersecurity and cyber diplomacy at an early stage, which it reflected in its strategic documents and successfully put into practice. The first cybersecurity strategy was issued in 2009, but was soon replaced in 2011 by a new strategy outlining the main guidelines, objectives and conditions for implementation over a five-year period. The title of the strategy is *Protecting and Promoting the UK in a Digital World.* The document[28] sets out four objectives, the second of which has a role to play in cyber diplomacy. The stated goal of the country is to be able to respond flexibly to cyber threats and attacks, and to be able to defend and enforce its interests

[26] Bundesamt für Sicherheit in der Informationstechnik.

[27] Federal Foreign Office: *Cyber Policy: Multilateral Solutions for the Future.* 25 September 2019.

[28] Cabinet Office: *The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital World.* November 2011.

more effectively in cyberspace. This presupposes proactive behaviour and active participation in the process of shaping cyberspace, the primary means of which are all peaceful: partly diplomatic and partly economic, as the British Government channels the commercial interests of British companies into the growing international cybersecurity market. The third cyber strategy, re-issued by the British Government on 1 November 2016 for another five years, is a significant step forward.[29] The document sets out three strategic goals – that is why we can call the 2016 cyber strategy the "3D strategy": 'defend, deter and develop' for the realisation of which it considers international action to be essential. In the second of the objectives, cyber diplomacy has a key role to play. Deterrence is envisaged not only by "hard" means (such as developing offensive cyber capabilities) but also by further broadening and deepening cooperation channels – as the strategy states: the British will continue to build on the global cyber alliance that has already begun and continue to support application of international law in cyberspace. Achieving the three strategic goals is only conceivable within an appropriate international framework. The U.K. continues to be at the forefront of creating a free, open, peaceful and secure cyberspace where international law is applicable and fundamental human rights are guaranteed both online and offline. In doing so, the U.K. is counting not only on its traditional allies, but also on its new partners, and is seeking to leverage the power of multilateral fora such as the UN, the G20, the European Union, NATO, the OSCE, the Council of Europe or the British Commonwealth.[30]

Bilateral cyber relations have a key role to play in achieving the goal of building a global cyber alliance. The *United States* is undoubtedly the number one country from among the British traditional allies with which the island nation has had a very close relationship on cyber issues for more than a decade in the context of the so-called "special relationship" – or as it has recently been called "the most important bilateral partnership". The need to involve private sector and business actors, research and development and the application of the basic institutions of the rule of law in cyberspace was already recorded in 2011.[31] In

[29] HM Government: *National Cyber Security Strategy 2016–2021.* United Kingdom, 01 November 2016.

[30] Dóra Molnár: Mérföldkövek a brit kiberbiztonság fejlődésében I. Az elméleti háttér megalapozása: a kiberbiztonsági stratégia [Milestones in the Development of the British Cyber Security I. Establishing the Theoretical Background: The Cyber Security Strategy]. *Hadmérnök,* 12, "KÖFOP" issue (2017). 144.

[31] Cabinet Office: *US–UK Cyber Communiqué.* 25 May 2011.

2015, President Obama and Prime Minister Cameron discussed the details of cooperation in Washington[32] which was finally institutionalised on 7 September 2016 by the cyber agreement signed by the two defence ministers.[33]

Although the U.K. has not yet signed a bilateral agreement with *China,* on 22 October 2015, during the Chinese President's visit to England, the two countries issued a joint statement on building their comprehensive global strategic partnership, launching the "Golden Age" of bilateral relations.[34] As part of this, it was stated that cyber actions aimed at unauthorised theft of intellectual property, trade secrets or confidential business information aimed at gaining a competitive advantage would not be conducted or supported against each other.[35]

Given the special partnership with the United States, it is not surprising that the United Kingdom also established bilateral cyber relations with Japan in 2012. The fifth stop of the biennial meetings was held in Tokyo on 31 January 2020.[36] Opportunities for capacity building and cooperation on the international stage were discussed during the meeting. This is in line with the main areas of cooperation identified at the fourth meeting in 2018, including support for a rules-based international cyber system and the sharing of national solutions for the safe use of IoT devices.[37]

Among the Asian bilateral relations, I would finally like to highlight *India,* which also has huge economic potential for the British – enough to think about the fact that the country already has 600 million Internet users and 650 million mobile users. An important aspect of India–U.K. security cooperation is cyber issues, and the India–U.K. cyber dialogue since 2012 has addressed issues such as cyber risk reduction, cybercrime management and building a global, multilateral, transparent and democratic system of Internet governance. In April 2018, the two countries signed in London a five-year framework agreement of cooperation in

[32] The White House: *Fact Sheet: U.S.–United Kingdom Cybersecurity Cooperation.* Office of the Press Secretary, 16 January 2015.

[33] Terri Moon Cronk: U.S.–U.K. Cyber Agreement Opens Doors for Both Nations. *DoD News,* 08 September 2016.

[34] For more details on some elements of the British China policy see U.K. Parliament: *The Making of UK Strategy towards China.* 04 April 2019.

[35] Foreign and Commonwealth Office: *UK–China Joint Statement 2015.* 22 October 2015.

[36] Ministry of Foreign Affairs of Japan: *The 5th Japan–UK Bilateral Consultations on Cyberspace.* 31 January 2020.

[37] Ministry of Foreign Affairs of Japan: *The 4th Japan–UK Bilateral Consultations on Cyberspace.* 16 March 2018.

14 areas. India has so far only concluded such a comprehensive cyber cooperation agreement with the United States outside the United Kingdom.[38]

The U.K. has already established bilateral cyber relations with a number of European countries. Of these, I highlight the Polish–British cyber cooperation agreement, not primarily because of its content (which is not a significant novelty), but because of its regional significance: through this relationship, the British want to support cyber capacity building programs in Eastern Europe and the Western Balkans.[39]

Finally, with regard to the United Kingdom, we must not forget the *Commonwealth,* which in itself is a long-standing diplomatic forum for the participating states, but in recent years the issue of cybersecurity has also been on the agenda on its own. The participating states institutionalised their cooperation on 20 April 2018 with the signing of the cyber declaration.[40] The declaration reaffirms the obligation of mutual assistance in building cyber capabilities and the need to formulate a common vision for cyberspace, which the U.K. is also financially supporting, contributing £15 million to the stated goals.[41]

Closing Remarks

The cyber preparedness of European states is also outstanding globally. This is well indicated by the Global Cybersecurity Index of the UN International Telecommunication Union (ITU) which provides a ranking of the cyber potential of states. According to the index, the U.K. is the world's leading cyber power, with France in third place. The third state surveyed, Germany, took 26th place.[42] It is very interesting, however, that in the fifth area examined, in terms of cooperation, the English have achieved a very good point, while France, a major diplomatic power, is lagging far behind. However, the examination of cybersecurity in Europe cannot end with a presentation of the three leading European states. There are many refreshing examples of how small countries can achieve great success in

[38] Rahul Roy-Chaudhury: India–UK Cybersecurity Cooperation: The Way Forward. *IISS,* 22 November 2019.

[39] Foreign and Commonwealth Office: *UK–Poland Cyber Co-operation Commitment.* 21 December 2017.

[40] The Commonwealth: *Commonwealth Cyber Declaration.* 20 April 2018.

[41] NCC Group: *Analysis: Untangling the Web of Multi-level Cyber Diplomacy.* 02 May 2018.

[42] UN ITU: *Global Cybersecurity Index 2018.* 2019.

cybersecurity. The index also reflects this, with Lithuania in 4th place and Estonia in 5th place in the overall world ranking. In addition, both states scored higher in the area of cooperation than the three leading major states. This result is a good indication of how small states place emphasis on the importance of cyber diplomacy and see the use of peaceful, diplomatic tools as superior to hard capabilities. In the case of Estonia, for example, it is no exaggeration to say that it has a global leadership role in cybersecurity. The headquarters of NATO and the EU are located in the capital of Estonia, where a number of international cyber arrangements have already been concluded. The small country's guiding role in organisational solutions is also evident: in the autumn of 2019, an independent cyber diplomacy unit was set up in the Ministry of Foreign Affairs, headed by ambassadors, with the task of representing the country in international organisations and fostering bilateral cyber relations – a model worth following.[43] Overall, the European area is at the forefront of the world in all its sub-issues, including cooperation, which could perhaps be the basis for laying the foundations for a peaceful cyberspace.

References

Agence nationale de la sécurité des systèmes d'information: *Défense et sécurité des systèmes d'information. Stratégie de la France.* 2011. Online: www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf

Agence nationale de la sécurité des systèmes d'information: *ANSSI/BSI Common Situational Picture.* Vol. 1 – July 2018. Online: www.ssi.gouv.fr/uploads/2018/07/bilateral-french-german-it-security-situation-report.pdf

Agence nationale de la sécurité des systèmes d'information: *Second Edition of the Franco–German Common Situational Picture.* 21 May 2019. Online: www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/D-F_Reports/Common_Situational_Picture_2019.pdf?__blob=publicationFile&v=2

Burgess, Christopher: Dissecting China's Global Bilateral Cybersecurity Strategy. *Security Boulevard,* 09 October 2016. Online: https://securityboulevard.com/2017/10/dissecting-chinas-global-bilateral-cybersecurity-strategy/

Cabinet Office: *US–UK Cyber Communiqué.* 25 May 2011. Online: www.gov.uk/government/publications/us-uk-cyber-communique

Cabinet Office: *The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital World.* November 2011. Online: www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

[43] E-Estonia: *Estonia Takes on a Major Role in Cyber Diplomacy with a New Department for International Cooperation.* 16 October 2019.

Chazan, Guy: German Cyber Security Chief Backs 5G 'No Spy' Deal over Huawei. *Financial Times,* 28 February 2020. Online: www.ft.com/content/5a0fe826-3b34-11e9-b856-5404d3811663
Consulat Général de France á Ekaterinbourg: *La diplomatie française à l'ère numérique.* 29 May 2019. Online: https://ru.ambafrance.org/La-diplomatie-francaise-a-l-ere-numerique
Cronk, Terri Moon: U.S.–U.K. Cyber Agreement Opens Doors for Both Nations. *DoD News,* 08 September 2016. Online: www.defense.gov/Explore/News/Article/Article/937878/us-uk-cyber-agreement-opens-doors-for-both-nations/
E-Estonia: *Estonia Takes on a Major Role in Cyber Diplomacy with a New Department for International Cooperation.* 16 October 2019. Online: https://e-estonia.com/estonia-cyber-diplomacy-international-cooperation/
Federal Foreign Office: *Cyber Policy: Multilateral Solutions for the Future.* 25 September 2019. Online: www.auswaertiges-amt.de/en/aussenpolitik/themen/multilateralism-cyber/2250332
Federal Ministry of the Interior: *Cyber-Sicherheitsstrategie für Deutschland 2016* [Cybersecurity Strategy for Germany 2016]. Online: www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf
Foreign and Commonwealth Office: *UK–China Joint Statement 2015.* 22 October 2015. Online: www.gov.uk/government/news/uk-china-joint-statement-2015
Foreign and Commonwealth Office: *UK–Poland Cyber Co-operation Commitment.* 21 December 2017. Online: www.gov.uk/government/publications/uk-poland-cyber-co-operation-commitment-joint-statement/uk-poland-cyber-co-operation-commitment
German Institute for International and Security Affairs: *Three Priorities for Cyber Diplomacy under the German OSCE Chairmanship 2016.* Berlin, 11 November 2015. Online: www.swp-berlin.org/en/point-of-view/three-priorities-for-cyber-diplomacy-under-the-german-osce-chairmanship-2016/
HM Government: *National Cyber Security Strategy 2016–2021.* United Kingdom, 01 November 2016. Online: www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
Laudrain, Arthur P. B.: France's New Offensive Cyber Doctrine. *Lawfare,* 26 February 2019. Online: www.lawfareblog.com/frances-new-offensive-cyber-doctrine
Ministère de l'Europe et des Affaires *Étrangères*: *Appel de Paris pour la confiance et la sécurité dans le cyberespace.* 12 November 2018. Online: www.diplomatie.gouv.fr/IMG/pdf/texte_appel_de_paris_-_fr_cle0d3c69.pdf
Ministère de l'Europe et des Affaires *Étrangères*: *Cybersécurité: Appel de Paris du 12 novembre 2018 pour la confiance et la sécurité dans la cyberespace. Liste des soutiens à l'appel de Paris (actualisé le 14 novembre 2018).* Online: www.diplomatie.gouv.fr/IMG/pdf/soutien_appel_paris_cle8e5e31.pdf
Ministère de l'Europe et des Affaires Étrangères: *Dinard Declaration on the Cyber Norm Initiative.* 06 April 2019. Online: www.diplomatie.gouv.fr/IMG/pdf/g7_dinard_declaration_on_cyber_initiative_cle4e553d.pdf
Ministère de l'Europe et des Affaires Étrangères: *Indo–French Bilateral Cyber Dialogue (Paris, 20 June 2019).* Online: www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/fight-against-organized-criminality/cyber-security/article/indo-french-bilateral-cyber-dialogue-20-06-19

Ministère de l'Europe et des Affaires Étrangères: *Inititative pour des normes dans le cyberespace. Synthese des enseignements tirés et des bonnes pratiques.* 26 August 2019. Online: www.diplomatie.gouv.fr/IMG/pdf/_fr_synthesis_cyber_norm_initiative_cle025b33.pdf

Ministère de l'Europe et des Affaires Étrangères: *Troisième dialogue stratégique France*–États-*Unis en matière de cybersécurité (Paris, 22 janvier 2020).* Online: www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/lutter-contre-la-criminalite-organisee/la-france-et-la-cybersecurite/actualites-et-evenements-lies-a-la-cybersecurite/article/troisieme-dialogue-strategique-france-etats-unis-en-matiere-de-cybersecurite-22

Ministère de l'Europe et des Affaires *Étrangères*: *La France et la cybersécurité.* s. a. Online: www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/la-france-et-la-cybersecurite/

Ministère des Armées: *Livre Blanc. Défense et sécurité nationale 2013.* Paris. Online: www.defense.gouv.fr/content/download/206186/2286591/file/Livre-blanc-sur-la-Defense-et-la-Securite-nationale%202013.pdf

Ministry of Foreign Affairs of Japan: *The 4th Japan–UK Bilateral Consultations on Cyberspace.* 16 March 2018. Online: www.mofa.go.jp/press/release/press4e_001960.html

Ministry of Foreign Affairs of Japan: *The 5th Japan–UK Bilateral Consultations on Cyberspace.* 31 January 2020. Online: www.mofa.go.jp/press/release/press4e_002766.html

Molnár, Dóra: Mérföldkövek a brit kiberbiztonság fejlődésében I. Az elméleti háttér megalapozása: a kiberbiztonsági stratégia [Milestones in the Development of the British Cyber Security I. Establishing the Theoretical Background: The Cyber Security Strategy]. *Hadmérnök,* 12, "KÖFOP" issue (2017). 136–148. Online: http://hadmernok.hu/170kofop_09_molnar.pdf

Nabeel, Fahad: International Cyber Regime: A Comparative Analysis of the US–China–Russia Approaches. *Stratagem,* 1, no. 2 (2018). 8–27. Online: www.academia.edu/38296708/International_Cyber_Regime_A_Comparative_Analysis_of_the_US-China-Russia_Approaches

NCC Group: *Analysis: Untangling the Web of Multi-level Cyber Diplomacy.* 02 May 2018. Online: www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/may/nalysis-untangling-the-web-of-multi-level-cyber-diplomacy/

Parameswaran, Prashanth: Singapore–Germany Cyber Cooperation in Focus with Introductory Visit. *The Diplomat,* 14 August 2018. Online: https://thediplomat.com/2018/08/singapore-germany-cyber-cooperation-in-focus-with-introductory-visit/

Rogusky, Przemyslaw: France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I. *Opinio Juris,* 24 September 2019. Online: http://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/

Roy-Chaudhury, Rahul: India–UK Cybersecurity Cooperation: The Way Forward. *IISS,* 22 November 2019. Online: www.iiss.org/blogs/analysis/2019/11/sasia-india-uk-cyber-security-cooperation

Sénat: *Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur la cyberdéfense.* Par le Sénateur M. Jean-Marie Bockel. Sénat session extraordinaire de 2011–2012. Enregistré á la Présidence du Sénat le 18 juillet 2012. Online: www.senat.fr/rap/r11-681/r11-6811.pdf

SGDSN: *La stratégie nationale pour la sécurité du numérique.* 2015. Online: www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf

SGDSN: *Revue stratégique de cyberdéfense.* 12 February 2018. Online: www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf
The Commonwealth: *Commonwealth Cyber Declaration.* 20 April 2018. Online: https://thecommonwealth.org/sites/default/files/inline/CommonwealthCyberDeclaration_1.pdf
The White House: *Fact Sheet: U.S.–United Kingdom Cybersecurity Cooperation.* Office of the Press Secretary, 16 January 2015. Online: https://obamawhitehouse.archives.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation
U.K. Parliament: *The Making of UK Strategy towards China.* 04 April 2019. Online: https://publications.parliament.uk/pa/cm201719/cmselect/cmfaff/612/61210.htm
UN ITU: *Global Cybersecurity Index 2018.* 2019. Online: www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
U.S. Department of State: *Joint Statement on U.S.–Germany Cyber Bilateral Meeting.* 24 March 2016. Online: https://2009-2017.state.gov/r/pa/prs/ps/2016/03/255082.htm
U.S. Department of State: *Joint Statement on Advancing Responsible State Behavior in Cyberspace.* 23 September 2019. Online: www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/

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.

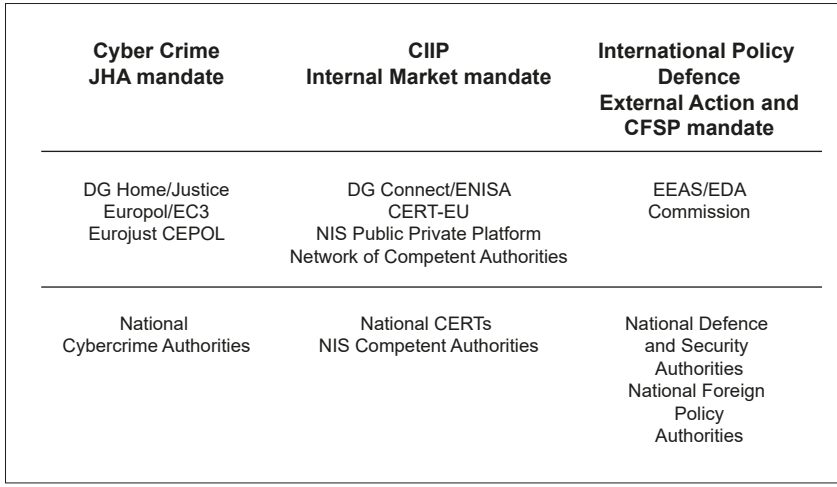

Figure 1. *The main pillars of the EU Cybersecurity Strategy*
Source: Christou (2016): op. cit.

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.

Csaba Krasznay

Case Study: The NotPetya Campaign

Introduction

The range of malicious acts affecting cyberspace is endless, but there are events that provide a red line and a point of reference for researchers. The attack on Estonia in 2007, the deployment of the Stuxnet malicious code, the leak of information by Edward Snowden were all such events when we had to re-evaluate our views on cyberspace. From the perspective of the present study, the NotPetya malicious code campaign is a turning point that explains the importance of international law and international relations in connection to cyber events. This incident has highlighted some critical points on the field of external relations, which showed in practice that the creation of the Tallinn Manual or the proposal for a Digital Geneva Convention was necessary because of the practice of some countries in interpreting international norms freely.

The Technical Perspective

According to a summary in the *Wired* magazine, the NotPetya campaign started on the afternoon of 27 June 2017, in the last working hours of the working day before the celebration of the Ukrainian Constitution. The date of the first infections was food for thought, as choosing a prominent holiday of the Republic of Ukraine as the beginning of the attack was a signal message. Meanwhile, at that moment it was still probable that the time was also chosen according to a plan based on the fact that the majority of IT operators would be on leave, so the defence would work with lower resources. Although the malware appeared soon in other countries, most of the infected machines were reported from Ukraine, so it is suspected that the target was Ukraine as a state and not some companies were on the crosshairs. In other countries, including Germany, France, Italy, Poland and the United States, there were only collateral damages. This theory is

https://doi.org/10.36250/01039_05

further reinforced by the fact that an explosive device hidden in a motor vehicle killed a member of the Special Forces in Kiev on the same day.[1]

The malicious code had the characteristics of a ransomware, encrypting the hard drive after infection, and asking for 300 USD in bitcoin in exchange for unlocking the machine. However, it soon became clear that the email address provided for the contact was not alive, so there was no chance of recovering the lost data. If the attack was financially motivated, as in the case of WannaCry a month before NotPetya, the attacker would have remained available and would have secured the return of the data in exchange for a ransom, as the victim only paid if there was a chance for the decryption as it was learnt from similar crimes. The characteristics of a ransomware in the early hours was also emphasised by the fact that the code showed similarities to the well-known Petya ransomware, but it was soon discovered that it was intentional camouflage, so the name NotPetya, or Non Petya, became widespread among cybersecurity experts.

In terms of mechanism of action, the malicious code infected the computer's master boot record, the hard disk segment responsible for loading the operating system, and began encrypting the file system after the machine was started. If that succeeded, it showed a typical ransomware message on the screen, indicating how much money it was asking for the decryption and how the communication was possible with the cybercriminals. Before making the machine unusable, it tried to spread to the network on which the infected machine was located. It used the EternalBlue vulnerability, and as it could be seen in case of WannaCry, it started to spread on the previously non-updated computers, meanwhile it collected the administrator password from the infected machine's memory, that also could give access to other networked machines.

The first infections were assumed to have come through a software update mechanism of the MEDoc application. This software is one of the officially approved tax return programs, so it runs on a significant part of Ukrainian companies. This program indicated that it needed to be updated, and then after the user allowed the patches to be installed, the infection began. There is no information on how they could influence the MEDoc update process. From remote hacking to direct, physical access to the update server, there are a number of possible solutions to consider. It seems certain that the attacker gained administrative privileges on one of MEDoc's servers, which allowed him to intervene in the

[1] Andy Greenberg: Petya Ransomware Epidemic May Be Spillover From Cyberwar. *Wired,* 28 June 2017.

update mechanism as well. According to an investigation by the cybersecurity company Talos, as early as 24 April 2017, an update was released to users that included a backdoor, so in principle, it allowed the attack to be carried out. Therefore, the attackers started preparing for the action months earlier. Against WannaCry, there was not any hidden code or so-called "kill switch", which would have enabled the rapid shutdown of the infection. The attacker's goal was clearly the largest, geographically most localised destruction.[2]

Eventually, thousands of Ukrainian companies were hit by the incident. The victims include certain critical Ukrainian infrastructures, including Ukrainian banks, the Kiev Borispol Airport, and energy companies such as Kyivenergo and Ukrenergo. But several foreign companies have also reported infections, such as the American medical company Merck, the Russian Rosnyeft and the Hungarian OTP Bank in Ukraine, whose ATMs displayed the images of the NotPetya infection for days. Most publicity was given to the devastation at A. P. Moller – Maersk. This company is the 558th largest conglomerate in the world according to the Forbes Global 2000 list of companies, one of the largest logistics companies in the world. The NotPetya infection reportedly made it impossible for the company to operate for two days. Loading of cargo ships worldwide had to be controlled manually, relying on paper and pencil instead of a computer. This was also reflected in the Danish company's revenue, with their quarterly report estimating that they suffered between $200 million and $300 million in damage from this two-day shutdown.[3]

International Law Perspective

The NotPetya malicious code is the first cyber incident that appears to be a coordinated attack on a sovereign state in peacetime, attacking its critical infrastructures, civilian facilities, causing additional damage to civilian companies operating in other countries as well. Its purpose was clearly destruction. Tools used by the malicious code were previously known, as neither the vulnerability exploited for network propagation nor the software that was used to access the credentials of privileged users caused a surprise to professionals. However, attack

[2] David Maynor et al.: The MeDoc Connection. *Talos Intelligence,* 05 July 2017.

[3] Maersk Press Room: *A. P. Moller – Maersk Improves Underlying Profit and Grows Revenue in First Half of the Year.* 16 August 2017.

tactics were completely new, preceded by a thorough operational planning, as the MEDoc software chosen for distribution was unknown beyond Ukraine, only adequate intelligence could confirm that this propagation vector could be so effective in carrying out a geographically focused cyberattack. The psychological or social engineering twist in the attack should also be emphasised, which led the victims to believe that a version of MEDoc that would open a backdoor for malicious code should be installed. For decades, cybersecurity professionals have been aware that both end-users and IT operators need to use the latest version of software, so if a software update is available, it should be installed as soon as possible. Therefore, the attacker built the distribution on this foundation, believing that users would install anything that appears to be an update as soon as possible, without question, so attacking the update server and using it as a distribution point is a brilliant choice.

From the states' perspective, the right answer should be decided if there is a cybersecurity incident that looks like a cyberwarfare activity, in which an advanced cyber weapon was deployed in a country that has previously suffered such targeted attacks and it is used regularly as a weapons test site by another country. Can it be said that this incident is classified as an attack within the meaning of international law? Can they use the means of attribution, or name a country an attacker? On the other hand, the question is also whether international diplomacy is prepared to deal with the countermeasures of the named country by traditional diplomatic means after such a declaration? Finally, the question is also whether the named attacking country can be put under pressure as a result of which it will reduce or end its hostilities in cyberspace?

Schmitt and Biller examined how the incident relates to the requirements of international law a few weeks after the NotPetya attack. Their first remark was that the malicious code was not reported to have caused injury or death. The author of the present study adds that, although no direct deaths were reported for either NotPetya or WannaCry, it cannot be excluded that non-functioning electronic information systems in some healthcare facilities, especially in case of WannaCry, may have contributed indirectly to deaths in the U.K. healthcare system that could have been prevented if the patient had been provided with appropriate care in a timely manner. Schmitt and Biller link accountability to attribution, i.e. the main question is whether the attack was backed by a country's armed forces, intelligence agencies, or whether the instructions were given by a state actor in case of a non-state attacker. Assuming that this has happened, a breach of three state obligations can be presumed. These are

respect for sovereignty, the principle of non-interference and the prohibition of the use of force.

According to Schmitt and Biller, sovereignty was violated during the NotPetya attack because of two conditions. On the one hand, a violation of territorial integrity, which in cyberspace can be imagined as an attack causing physical damage or personal injury, possibly death. In a broad interpretation, if a cyber infrastructure becomes unavailable for an extended period of time, in the opinion of the authors, a violation of territorial integrity can also be formulated. Because NotPetya went beyond the effects of an average distributed denial of service attack, specifically involving the loss of key data and the need to deploy new machines instead of disrupted critical computer systems, this can be seen as damage to physical facilities. The other condition would be the disruption of core government activities, but this was not the case for NotPetya. Although the IT systems that enable financial institutions to operate are damaged, they do not support basic government functionality, so this condition for violating sovereignty did not exist.

Violations of the principle of non-interference are accompanied by coercive actions taken by one state against another in order to change its political, economic, social and cultural order and to influence foreign policy. Schmitt and Biller did not see evidence that the NotPetya malicious code was capable of achieving these purposes, given that its purpose was destruction and not influence. If the cyber weapon had indeed been a ransomware virus, which seemed at first glance, coercion would in principle have been possible since the essence of ransom is to extort some decision from the other party.

The principle of the use of force in peacetime means that a state engages in a violent activity that does not qualify as self-defence or collective defence without a UN mandate. Activities in the cyberspace typically have little impact on the physical environment, making it difficult to imagine an attack that reaches an unauthorised level of use of force. The long-term outage of a cyber infrastructure as computers or network devices become inaccessible due to a malicious code like NotPetya, however, could be classified as unauthorised use of force. According to the authors, economic destabilisation may also fall into this category. According to the Ukrainian Government, the cyberattack has reached this level, but international practice in mid-2017 has not yet provided a clear answer as to where the threshold is.

The authors' opinion is that international humanitarian law would be valid in this case if there were an international armed conflict between two states, namely

Ukraine and, suppose, Russia. The condition in that case is that one country occupies the territory of another country or supports a non-state group that engages in hostile activity against the other country. Given the support of the Crimean Peninsula and the uprisings in eastern Ukraine, the authors see a legitimate presumption of an armed conflict between the two states, therefore the use of NotPetya should also be examined under international humanitarian law, despite the fact that in the UN GGE there is no full agreement on this.[4] The classification of this malicious code should be examined in the light of the Tallinn Handbook, which states that the use of such cyber weapons is an attack even if it does not directly damage the cyber infrastructure, only has indirect effects. According to some experts, the inaccessibility of such infrastructure also belongs to that set.

NotPetya's targets included the Kiev Airport, the Chernobyl power plant, and the Ukrainian healthcare system. If it can be assumed that this was done in accordance with the attacker's intention and not due to the uncoordinated spread of the malicious code, this can be classified as an attack according to the authors. Although some of the disputed facilities could be classified as dual use, such as the airport, most elements of cyber infrastructure are clearly civilian, not serving military purposes, so the act could even fall into the category of a war crime. In addition, the impact of cyber weapons went beyond Ukraine, it also had an impact on third countries, so their neutrality was violated by the attacker.[5]

All of these are, of course, only the scientific thinking of researchers, as mentioning war crimes in case of a cyberattack can have serious diplomatic implications, if it is done by a politician in charge. As it can be read in the next chapter, states use moderate expressions, even if they have a strong diplomatic reaction. NotPetya, on the other hand, is special that in addition to researcher positions, there have been comments and then political resolutions that should be taken more seriously than theoretical reasoning. First, researchers from NATO's Center for Excellence in Cooperative Cyber Defense analysed the situation. The quoted Michael Schmitt also belongs to this scientific circle, but the analysis quoted earlier did not appear on the organisation's website, therefore the article by Blumbergs, Minárik, van der Meij and Lindström has already been published by the world press as NATO's position. Thus, special emphasis is placed on what Minárik said:

[4] Michael N. Schmitt – Liis Vihul: International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms. *Just Security,* 30 June 2017.

[5] Michael N. Schmitt – Jeffrey Biller: The NotPetya Cyber Operation as a Case Study of International Law. *EJIL:Talk!,* 11 June 2107.

"If the operation is related to an international armed conflict, it is subject to the legislation on armed conflict." Previously, NATO CCD COE commentaries had not visited the world press on such a delicate matter, so it could be perceived that NotPetya weighed significantly more than any other previous case.[6]

The States' Answer

Countries were not prepared for such a serious violation of international norms. The really big breakthrough came only in February 2018, when 7 countries, the United States, the United Kingdom, Denmark, Lithuania, Estonia, Canada and Australia, jointly condemned Russia for the NotPetya attack, which was officially supported by New Zealand, Norway, Latvia, Sweden and Finland. Never before have several countries used the means of attribution together, that is, they have pointed out the attacker in unison. Attribution is always a political decision that can be supported by technical or intelligence evidence, but without political will, they are not worth much. Tobias Feakin, Australia's Ambassador for Cyber Affairs, summed up excellently why this joint stand was an important step and what it means for the attackers:

> "What we're doing is maturing this approach in order that the consequences will be felt further in the future. So another key part of deterrence is signalling to another country, to provide clear, consistent, and credible messaging to adversaries that there will be repercussions for the behaviour that they're conducting."[7]

Depending on the attribution's certainty, there are several tools in the hand of nation states to give answer to a cyberattack. Moret and Pawlak give an example, how individual countries or EU institutions, member states in the EU Council or the EU in cooperation with international organisations can choose from the following answers:

- statements and demarches
- international agreements

[6] Bernhards Blumbergs et al.: NotPetya and WannaCry Call for a Joint Response from International Community. *NATO CCD COE,* 2017.

[7] Stilgherrian: Blaming Russia for NotPetya was Coordinated Diplomatic Action. *ZDNet,* 11 April 2018.

- capacity building
- strategic communication
- joint investigations
- statements by HR/VP
- EU demarches
- formal request for assistance
- Council conclusions
- political and cyber dialogues
- recalling diplomats
- sanctions
- solidarity clause
- countermeasures
- Mutual Defence Clause
- military response[8]

At the time of NotPetya only the United States implemented unilateral cyber sanctions. In 2015, President Barack Obama used this format against North Korea in response to the attack against Sony Pictures. Therefore, other countries have not had any tested and proven responses against devastating cyberattacks. Until 2017, most countries officially treated the threats in cyberspace as an internal defence question; however, they agreed that international norms and legislation are valid in the cyberspace as well. Attribution, diplomatic or even military responses were not part of the common diplomacy toolbox. Only the United States had enough power to publicly attribute another country, generally speaking Russia, Iran and North Korea in connection with cyberattacks. That is why NotPetya was a game changer. The U.S. Government attributed the NotPetya attack to Russia with the following statement from the Press Secretary of the White House:

> "In June 2017, the Russian military launched the most destructive and costly cyber-attack in history. The attack, dubbed "NotPetya," quickly spread worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas. It was part of the Kremlin's ongoing effort to destabilize Ukraine and demonstrates ever more clearly Russia's involvement in the ongoing conflict. This was also a reckless and indiscriminate cyber-attack that will be met with international consequences."[9]

[8] Erica Moret – Patryk Pawlak: The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime? *EUISS,* July 2017.

[9] The White House: *Statement from the Press Secretary.* 15 February 2018.

The Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security (DHS) together with the Federal Bureau of Investigation (FBI) even created a separate investigation and attribution stream to the Russian cyberattacks. It is called Grizzly Steppe. Both agencies analyse the tactics, techniques and procedures (TTPs as it is used in cybersecurity) of Russian state sponsored actors. Codename Grizzly Steppe was chosen right after the alleged intervention of Russian secret services in the 2016 Presidential Election. The list of cyberattacks was later enhanced with NotPetya and the cyber activity of the Russian Government targeting energy, other critical infrastructure sectors and network infrastructure devices.[10] DHS summarised such activities with the following sentences:

> "Russia's civilian and military intelligence services engaged in aggressive and sophisticated cyber-enabled operations targeting the U.S. government and its citizens. The U.S. Government refers to this activity as GRIZZLY STEPPE. These cyber operations included spearphishing campaigns targeting government organizations, critical infrastructure entities, think tanks, universities, political organizations, and corporations, and theft of information from these organizations. This stolen information was later publicly released by third parties. In operations targeting other countries, including U.S. allies and partners, Russian intelligence services (RIS) have undertaken damaging or disruptive cyber-attacks, including on critical infrastructure—in some cases masquerading as third parties or hiding behind false online personas designed to cause the victim to misattribute the source of the attack."[11]

Such approach is not surprising from the United States. It uses a very straight diplomatic language against its main global competitors and especially in cyber cases, it always tries to clarify the boundaries of acceptable international norms. Until the 2015 meeting of President Barack Obama and President Xi Jinping when the two leaders agreed on major cybersecurity questions, U.S. officials mainly remembered about the unacceptable behaviour of China. Later on, the U.S. seemingly forgot China and turned to Russia. In 2020, the U.S. criticises China again, following its general foreign policy.

A similar approach can be seen in other countries. Close U.S. allies like the United Kingdom or Australia also had clear statements on NotPetya. On

[10] Cybersecurity and Infrastructure Security Agency: *Grizzly Steppe – Russian Malicious Cyber Activity.* 16 April 2018.

[11] Department of Homeland Security: *Executive Summary of Grizzly Steppe Findings from Homeland Security Assistant Secretary for Public Affairs Todd Breasseale.* 30 December 2016.

15 February 2018, U.K. Foreign Office Minister Lord Ahmad attributed this cyberattack to Russia highlighting that the U.K. and its allies will not tolerate malicious cyber activities.

> "The UK Government judges that the Russian Government, specifically the Russian military, was responsible for the destructive NotPetya cyber-attack of June 2017. The attack showed a continued disregard for Ukrainian sovereignty. Its reckless release disrupted organisations across Europe costing hundreds of millions of pounds. The Kremlin has positioned Russia in direct opposition to the West yet it doesn't have to be that way. We call upon Russia to be the responsible member of the international community it claims to be rather then secretly trying to undermine it. The United Kingdom is identifying, pursuing and responding to malicious cyber activity regardless of where it originates, imposing costs on those who would seek to do us harm. We are committed to strengthening coordinated international efforts to uphold a free, open, peaceful and secure cyberspace."[12]

The United Kingdom, part of the Five Eyes countries and closest ally of the U.S. is also very straight with Russia; unsurprisingly, Russia has many active operations on the island.

On the next day, 16 February 2018, Australian Minister for Law Enforcement and Cyber Security, Angus Taylor released the following statement:

> "Australian Government attribution of the 'NotPetya' cyber incident to Russia. The Australian Government has joined the governments of the United States and the United Kingdom in condemning Russia's use of the 'NotPetya' malware to attack critical infrastructure and businesses in June 2017. Based on advice from Australian intelligence agencies, and through consultation with the United States and United Kingdom, the Australian Government has judged that Russian state sponsored actors were responsible for the incident. Computers were infected by a sophisticated piece of malware – or malicious software – that masqueraded as ransomware. 'NotPetya' interrupted the normal operation of banking, power, airports and metro services in Ukraine. While the brunt of the impact was felt in Ukraine, the malware spread globally, affecting a number of major international businesses causing hundreds of millions of dollars in damage. The Australian Government condemns Russia's behaviour, which posed grave risks to the global economy, to government operations and services, to businesses activity and the safety and welfare of individuals. The Australian Government is further strengthening its international partnerships through an International Cyber Engagement Strategy to deter and respond to the malevolent use of cyberspace. The Government is committed to ensuring the Australian public sector, businesses and the community are prepared for evolving cyber threats."[13]

[12] Foreign and Commonwealth Office: *Foreign Office Minister Condemns Russia for NotPetya Attacks.* 15 February 2018.

[13] Parliament of Australia: *Australian Government Attribution of the 'NotPetya' Cyber Incident to Russia.* 16 February 2016.

Australia is more exposed to Chinese cyberattacks, therefore it rarely deals with Russian originated attacks. We can treat this remark as a polite gesture for the United States.

Estonian Minister of Foreign Affairs, Sven Mikser reflects to the U.K. Government in his press release:

> "The NotPetya cyber-attack which targeted Ukraine's financial, energy and government sectors and undermined the sectors' resilience, demonstrated disrespect for Ukrainian sovereignty and caused significant economic losses in other countries too. It is very important for Estonia to maintain an open, stable and secure cyber space and for that, countries have to act responsibly and follow the rules of international cooperation and the norms of international law that apply in cyber space just like everywhere else."[14]

Estonia is the closest ally of the United States in the Baltic region and has the closest ties towards the U.S. in cybersecurity. They were also the first country that suffered a devastating cyberattack from Russia. Estonians are also pioneering in cyber diplomacy. It is not surprising that that full support was given for the attribution.

As we can see, those countries who officially attributed the cyberattack to Russia, draw up their views by the foreign ministers or ministers responsible for cybersecurity. Supporting nations of this diplomatic step also emphasised the role of Russia, but the announcements were made by lower ranked government officials. For example, in New Zealand, Director-General of the Government Communications Security Bureau (GCSB) Andrew Hampton released the statement.

> "While NotPetya masqueraded as a criminal ransomware campaign, its real purpose was to damage and disrupt systems […]. Its primary targets were Ukrainian financial, energy and government sectors. However, NotPetya's indiscriminate design caused it to spread around the world affecting these sectors world-wide. While there were no reports of NotPetya having a direct impact in New Zealand, it caused disruption to some organisations while they updated systems to protect themselves from it. This reinforces that New Zealand is not immune from this type of threat. In a globally connected world our relative geographic isolation offers no protection from cyber threats. We support the actions of our cyber security partners in calling out this sort of reckless and malicious cyber activity."[15]

[14] Republic of Estonia: *Foreign Minister Mikser Condemns Russia for NotPetya Attacks against Ukraine.* 15 February 2018.

[15] Government Communications Security Bureau: *New Zealand Joins International Condemnation of NotPetya Cyber-attack.* 16 February 2018.

New Zealand, like Australia is far from Russia and has much more problems in the cyberspace with China. As member of the Five Eyes countries, it supported the attribution, but we can assume that the government has not given high priority for this issue.

In case of Latvia, the public reaction was a short message on Twitter from the Ministry of Foreign Affairs: "#Latvia is deeply concerned about the findings of UK & US attribution of #NotPetya #Cyber_attacks and stands for responsible state behaviour in cyberspace." In case of a country with 27% of native Russians, even a tweet can be a strong support towards its NATO allies.

Deterrence in Cyberspace

NotPetya was the red line for Western countries that invoked not only diplomatic reactions as it was mentioned in the previous section, but after 2018, some countries, especially the United States have publicly introduced some retaliatory actions against Russia. This is not surprising as according to the traditional deterrence theory, three elements should be present to stop a rogue activity: attribution, credible signalling and deterrence strategies. Taddeo explains that as follows:

> "A believes that B is planning to attack it. In order to avoid the attack, A makes an explicit commitment to take action against B, should B decide to attack. A's commitment should be such that B is convinced that any action against A will fail, because A has the capacity either to resist or punish B, and to outweigh any prospective gains for B. B's conviction hinges on A's signalling and credibility to act as it threatens. According to this model, we find here the three core elements of deterrence theory: the identification of the opponent (attribution); defence and retaliation as types of deterrence strategies; and the capability of the defender to signal credible threats."[16]

In that sense, attribution is only the first step. However, responsible attribution is not as easy as it seems to be, that is why only the United States, the only superpower used this tool before NotPetya. In the cyberspace, attribution needs both convincing technical evidence and reliable intelligence sources. Due to the anonym and global nature of the Internet, collection of hard evidence from computers and networks is struggling. What can be seen on the defenders' side is only a few technical information or indicators of compromise (IoC). They are usually files and operating system

[16] Mariarosaria Taddeo: The Limits of Deterrence Theory in Cyberspace. *Philosophy and Technology,* 31, no. 3 (2018). 339–355.

activities or source/destination IP addresses. Security researchers should prove who are behind NotPetya by finding evidence in the following infection process:

- dropped files
- process hashes and process privilege checks
- credential theft
- token impersonation
- malware propagation
  - network node enumeration
  - SMB copy and remote execution
  - SMBv1 exploitation via EternalBlue
- UNC write malware to admin$ on remote target
- remote execution of the malware
  - MBR ransomware
  - physical drive manipulation
  - MFT encryption
- file encryption
- system shutdown
- anti-forensics[17]

In case of NotPetya, the EternalBlue vulnerability, used for malware propagation was originated from the National Security Agency in the United States. For credential theft, the attackers used Mimikatz, originally created as a proof of concept by French security researcher Benjamin Delpy in 2011. There was not a complex network infrastructure with millions of previously infected computers in the botnet, as the attack was targeted, originated from the MEDoc update server and it is still not known who and how has hacked this server. In such cases, researchers can only rely on the coding style of the malware. Source codes are similar to fingerprints. A programmer usually has his own coding style, a group of programmers are usually using the same framework to improve their software. Cybercriminals are usually lazy enough to make only minor changes, "feature releases" in different campaigns. But that is not true in case of sophisticated, state sponsored targeted attacks. The name NotPetya was chosen as for first sight, it was similar to Petya ransomware, although it is now obvious, that there is no connection between the two malwares. It is possible that the original source code of NotPetya was stolen or bought from the original author

[17] Karan Sood – Shaun Hurley: NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft. *Crowdstrike,* 29 June 2017.

who was convicted by a regional court in Nikopol in the Dnipropetrovsk Oblast of Ukraine to one year in prison in 2018 after pleading guilty to having spread a version of Petya online. He is an unnamed Ukrainian citizen.

NotPetya's traces were well-hidden from the technical perspective. Neither governmental, nor industry sources have uncovered any "smoking guns" that underpins the role of Russia in this cyberattack. However, many countries attributed them with high confidence. We can assume that the United States and maybe other countries had indisputable intelligence information. As Carr wrote:

> "The most likely adversary responsible for a covert attack against those critical systems is an extremist group (religious, political, or anarchist), and the best way to learn which of those groups may have been responsible post-attack is to already have in place a long-term counter-intelligence campaign of infiltration and the development of trusted contacts with access. This cannot be done virtually or from behind a computer. Rather, those intelligence agencies that have yet to devote the bulk of their budget to signals capabilities may be best positioned to tackle the problem of attribution. They understand the need to continue to fund and even expand human intelligence – this is still vital, despite the fact that we are living in the age of Facebook, Twitter and Instagram."[18]

The assumption about the U.S. and allies' capabilities on cyber intelligence against Russia can be confirmed with some examples after NotPetya. We can count such leaked information and direct responses as credible signalling according to the deterrence theory. As Taddeo defines:

> "Signaling can be either general or tailored. General signaling conveys a message about the overall deterrence strategy to the rest of the international arena, through open statements released by a state conveying information about its approaches, commitments, and capabilities. […] Tailored signalling—the conveying of a threat to a specific offender indicating the possible targets of retaliation—is more problematic than general signalling and constitutes a significant obstacle to delivering effective deterrence strategies in cyberspace. This kind of signalling is effective if attribution is certain. If the defender has not identified the offender correctly, tailored signalling can be counterproductive given it may be directed to the wrong actor. Tailored signalling also requires a careful finetuning in order not to expose the defender's capabilities and assets, especially when the defender is considering retaliation in-kind. The risks are multiple and range from exposing knowledge about the opponent's cyber assets, which would imply that the defender has also run cyber operations (sabotage or espionage) against the opponent, to revealing the defender's assets and strategies, which may expose and therefore render futile its cyber capabilities, such as zero-day exploits (for example)."[19]

[18] Jeffrey Carr: Responsible Attribution: A Prerequisite for Accountability. *NATO CCD COE,* 2014.
[19] Taddeo (2018): op. cit. 352.

First of all, on 11 June 2018, the U.S. Department of Treasury's Office of Foreign Assets Control designated five Russian entities and three Russian individuals under Executive Order (E.O.) 13694, *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities.* All property and interests in property of the designated persons subject to U.S. jurisdiction are blocked, and U.S. persons are generally prohibited from engaging in transactions with them.[20]

Some notable cyberattacks can also show how Western countries retaliated Russian cyber (and other military) activities by flashing their capabilities:

- Panama Papers: On 1 April 2016, Mossack Fonseca, Panamanian law firm and corporate service provider notified its customers that millions of digital documents were stolen after a targeted cyberattack. These documents consisted of detailed information about the tax avoidance and money laundry of many notable persons. The hack was committed by an unknown hacker, "John Doe", who said that he had never worked for any intelligence agency. Whether it is true or not, the *Süddeutsche Zeitung* published an interview with Alexey Navalny, head of the Moscow-based NGO Anti-Corruption Foundation on the connection of President Putin and other leading figures with the Panama Papers.
- Dutch intelligence against Cozy Bear: In January 2018, Dutch news sources published a story on how their domestic intelligence service, AIVD accessed the IT system of the Cozy Bear hacker group, that is believed to be associated with Russian intelligence. This group is suspected with many notable cyberattacks, such as attacks during the 2016 Presidential Election.
- Bellingcat and Skripal Poisoners: In 2018 and 2019, Bellingcat, the online investigative journal has published a series of articles about the poisoners of Sergei Skripal and his daughter, who died in the United Kingdom. Based on open source intelligence, they could identify the poisoners and track back their lives even until high school. Although such investigative journalism is highly appreciated, it can be assumed that some kind of official intelligence support was provided by Western countries.
- U.S. cyberattacks on Russian Power Grid: In response to the cyberattacks against its critical infrastructures, the U.S. has conducted a similar attack and shared this information with the press in June 2019. As President Trump's national security adviser, John R. Bolton said, the United States

[20] U.S. Department of Treasury: *Treasury Sanctions Russian Federal Security Service Enablers.* 11 June 2018.

was now taking a broader view of potential digital targets as part of an effort "to say to Russia, or anybody else that's engaged in cyberoperations against us, 'You will pay a price'."

Conclusion

Traditional deterrence theory proposes two potential deterrence strategies: deterrence by defence and by retaliation. In the cyberspace, believing solely in deterrence by defence is not a real option. Simply, because the already developed tools, techniques and procedures set are enormous, and attackers can easily create a previously non-existing attack path. From their point of view, one weak link in the defence chain is enough for success. Therefore, countries should rely more on defence by retaliation, not forgetting to improve their defence capabilities as well. We can see such efforts all over the world.

The EU Cyber Diplomacy Toolbox is an example for that. As the press release of the Council of the EU states:

> "On 17 May 2019, the Council established a framework which allows the EU to impose targeted restrictive measures to deter and respond to cyber-attacks which constitute an external threat to the EU or its member states, including cyber-attacks against third States or international organizations where restricted measures are considered necessary to achieve the objectives of the Common Foreign and Security Policy (CFSP)."[21]

The lack of EU reaction to NotPetya is a symptom why this Toolbox is necessary. As the relation of the EU members to Russia is complicated, without such common understanding, it is difficult to find a harmonised way for joint sanctions. But states do not forget and forgive. After 5 years of a cyberattack against the German Parliament, Chancellor Angela Merkel seeks EU sanctions as they have hard evidence against Russian actors. This will be the first test of the Toolbox where EU members can prove their willingness for a coordinated response.[22]

> "Cyber-attacks falling within the scope of this new sanction's regime are those which have significant impact and which:

[21] Council of the EU: *Cyber-attacks: Council Is Now Able to Impose Sanctions.* 17 May 2019.
[22] Catherine Stupp: Germany Seeks EU Sanctions for 2015 Cyberattack on Its Parliament. *The Wall Street Journal,* 11 June 2020.

> – originate or are carried out from outside the EU or
> – use infrastructure outside the EU or
> – are carried out by persons or entities established or operating outside the EU or
> – are carried out with the support of person or entities operating outside the EU
> Attempted cyber-attacks with a potentially significant effect are also covered by this sanction's regime. […] Restrictive measures include a ban on persons travelling to the EU, and an asset freeze on persons and entities. In addition, EU persons and entities are forbidden from making funds available to those listed."[23]

We can see that the U.S. Government is actively using deterrence by retaliation strategy. Currently, it seems to be successful, as since 2017 there was not any major cyberattack, attributed to Russia. However, most of the actions on that field are covert and the public audience will get information decades later. Jason Healey, one the best scholars in this topic and Neil Jenkins tried to measure the success of deterrence from the U.S. perspective. Their article ends with the following thoughts:

> "We can't assess what we don't try to measure. Together, the frameworks in this paper can act as a check on whether these new, riskier U.S. cyber policies and operations are succeeding in suppressing incoming attacks, or inciting them. […] the U.S. Government cannot easily even know all its own operations against adversaries: some will be covert actions, others espionage, while others are "traditional military operations." Each is held in a separate compartment and few individuals have the full picture."[24]

Whatever will happen, the alleged attackers' response will be the same as what we heard from Kremlin spokesman Dmitry Peskov in February 2018, right after the attribution of many countries: "We categorically reject such accusations. We consider them unsubstantiated and groundless. This is nothing but a continuation of a Russophobic campaign that is not based on any evidence."[25]

NotPetya was nor the first, neither the last cyberattack in history. Countries should develop acceptable norms and behaviour in cyberspace, but they are getting farther and farther from a consensus. As both Russia and China can be more independent from the U.S. governed global Internet, as members of the

[23] Council of the EU (2019): op. cit.

[24] Jason Healey – Neil Jenkins: Rough-and-Ready: A Policy Framework to Determine if Cyber Deterrence is Working or Failing. In Tomáš Minárik – Siim Alatalu – Stefano Biondi – Massimiliano Signoretti – Ihsan Tolga – Gábor Visky (eds.): *11th International Conference on Cyber Conflict: Silent Battle.* Tallinn: NATO CCD COE Publications, 2019. 123–142.

[25] AFP: Kremlin 'Categorically' Denies Russia behind NotPetya Cyber-attack. *France 24,* 15 February 2018.

United Nations Security Council, they are able, and they are willing to influence where the cyberspace is turning. As of 2020, we can see a clear intention from the Western countries to sustain the current situation and remarkable steps from Russia and China towards changing it. Diplomats of the 2020s should notice that what is happening today will have a fundamental effect for the next five decades.

References

AFP: Kremlin 'Categorically' Denies Russia behind NotPetya Cyber-attack. *France 24,* 15 February 2018. Online: www.france24.com/en/20180215-kremlin-categorically-denies-russia-behind-notpetya-cyber-attack

Blumbergs, Bernhards – Tomáš Minárik – Kris Van Der Meij – Lauri Lindström: NotPetya and WannaCry Call for a Joint Response from International Community. *NATO CCD COE,* 2017. Online: https://ccdcoe.org/news/2017/notpetya-and-wannacry-call-for-a-joint-response-from-international-community/

Carr, Jeffrey: Responsible Attribution: A Prerequisite for Accountability. *NATO CCD COE,* 2014. Online: https://ccdcoe.org/uploads/2018/10/Tallinn-Paper-No-6-Carr.pdf

Council of the EU: *Cyber-attacks: Council Is Now Able to Impose Sanctions.* 17 May 2019. Online: www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/

Cybersecurity and Infrastructure Security Agency: *Grizzly Steppe – Russian Malicious Cyber Activity.* 16 April 2018. Online: www.us-cert.gov/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity

Department of Homeland Security: *Executive Summary of Grizzly Steppe Findings from Homeland Security Assistant Secretary for Public Affairs Todd Breasseale.* 30 December 2016. Online: www.dhs.gov/news/2016/12/30/executive-summary-grizzly-steppe-findings-homeland-security-assistant-secretary

Foreign and Commonwealth Office: *Foreign Office Minister Condemns Russia for NotPetya Attacks.* 15 February 2018. Online: www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks

Government Communications Security Bureau: *New Zealand Joins International Condemnation of NotPetya Cyber-attack.* 16 February 2018. Online: www.gcsb.govt.nz/news/new-zealand-joins-international-condemnation-of-notpetya-cyber-attack/

Greenberg, Andy: Petya Ransomware Epidemic May Be Spillover From Cyberwar. *Wired,* 28 June 2017. Online: www.wired.com/story/petya-ransomware-ukraine/

Healey, Jason – Neil Jenkins: Rough-and-Ready: A Policy Framework to Determine if Cyber Deterrence is Working or Failing. In Tomáš Minárik – Siim Alatalu – Stefano Biondi – Massimiliano Signoretti – Ihsan Tolga – Gábor Visky (eds.): *11th International Conference on Cyber Conflict: Silent Battle.* Tallinn: NATO CCD COE Publications, 2019. 123–142.

Maersk Press Room: *A. P. Moller – Maersk Improves Underlying Profit and Grows Revenue in First Half of the Year.* 16 August 2017. Online: www.maersk.com/press/

press-release-archive/20170816-a-p-moller-maersk-improves-underlying-profit-and-grows-revenue-in-first-half-of-the-year
Maynor, David – Aleksandar Nikolic – Matt Olney – Yves Younan: The MeDoc Connection. *Talos Intelligence,* 05 July 2017. Online: https://blog.talosintelligence.com/2017/07/the-me-doc-connection.html
Moret, Erica – Patryk Pawlak: The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime? *EUISS,* July 2017. Online: www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf
Parliament of Australia: *Australian Government Attribution of the 'NotPetya' Cyber Incident to Russia.* 16 February 2018. Online: https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22media%2Fpressrel%2F5793917%22
Republic of Estonia: *Foreign Minister Mikser Condemns Russia for NotPetya Attacks against Ukraine.* 15 February 2018. Online: https://vm.ee/en/news/foreign-minister-mikser-condemns-russia-notpetya-attacks-against-ukraine
Schmitt, Michael N. – Jeffrey Biller: The NotPetya Cyber Operation as a Case Study of International Law. *EJIL:Talk!,* 11 June 2107. Online: www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/
Schmitt, Michael N. – Liis Vihul: International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms. *Just Security,* 30 June 2017. Online: www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/
Sood, Karan – Shaun Hurley: NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft. *Crowdstrike,* 29 June 2017. Online: www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/
Stilgherrian: Blaming Russia for NotPetya was Coordinated Diplomatic Action. *ZDNet,* 11 April 2018. Online: www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/
Stupp, Catherine: Germany Seeks EU Sanctions for 2015 Cyberattack on Its Parliament. *The Wall Street Journal,* 11 June 2020. Online: www.wsj.com/articles/germany-seeks-eu-sanctions-for-2015-cyberattack-on-its-parliament-11591867801
Taddeo, Mariarosaria: The Limits of Deterrence Theory in Cyberspace. *Philosophy and Technology,* 31, no. 3 (2018). 339–355. Online: https://doi.org/10.1007/s13347-017-0290-2
The White House: *Statement from the Press Secretary.* 15 February 2018. Online: https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/
U.S. Department of Treasury: *Treasury Sanctions Russian Federal Security Service Enablers.* 11 June 2018. Online: https://home.treasury.gov/news/press-releases/sm0410

Anita Tikos

Cyber Diplomacy and the V4 Countries

Introduction

If we think about diplomacy, it is commonly understood as a task of the Ministries of Foreign Affairs to influence decisions, conduct dialogues and negotiations between representatives of states or international groups, forums. Due to the digital development, in the 21st century, the use of IT solutions and tools in diplomatic services became more and more widespread starting from public relations and information sharing, to data collection for intelligence purposes. In view of all this, it is more and more important to establish common rules, code of conducts, security related requirements within the cyberspace.

We can find several different meanings and definitions for cyber diplomacy. In this article, cyber diplomacy is understood, when country representatives (not only form the Ministry of Foreign Affairs, but from any governmental cyber related institution) share information, conduct dialogues or negotiations regarding any cybersecurity related topic (about an incident, about existing regulatory or organisational experiences, common EU regulations, exercises, etc.) in general (not going deeply into restricted or sensitive technical details).

The Central European Cyber Security Platform (CECSP) is a regional cooperation where members use strategic cooperation or cyber diplomacy to get the necessary information, experience or knowledge from the other countries and to get enough support to be able to effectively promote their interests in the bigger international communities.

First, I would like to introduce the development of the international forums and cooperation to get a full picture about the colourful palette of the different international cooperation platforms and forums where CECSP was born.

In the last decade, cybersecurity has appeared as a key challenge for all countries and organisations, resulting in the establishment of organisations or divisions that are responsible for the creation and maintenance of information

https://doi.org/10.36250/01039_06

security (e.g. authorities, CSIRTs,[1] Security Operation Centres, cyber defence agencies or centres of excellence, etc.). Due to the possible cross-border nature of threats and incidents, it became relatively clear at an early stage that there is a need for international forums and mechanisms for the structured international cooperation of the specialised IT security organisations.

Regarding cybersecurity, cooperation is one of the most important and at the same time the most challenging issues for every country. Although it is essential for all entities in the cyberspace to get relevant information on the latest threats but giving such threat intelligence for others usually encounters obstacles because of several aspects (for example national and security interest, data protection aspects etc.).

First, a technical international cooperation has been established by setting up communities of incident management centres (CERT[2]/CSIRT); after the CSIRT communities the political, strategic cooperation has been established in different forms (groups of authorities, strategic working groups by decision-makers, etc.). As of today, the main international organisations (NATO, EU, ITU, OSCE) all put cybersecurity on their agenda.

This wide list of international cooperation is always growing because of the different cooperation models (who are the involved players) and because of the developing technology (technology creates new and new policy areas) as well.

In 2013, the Czech Republic and Austria has enriched this huge cooperation with initiating the establishment of the Central European Cyber Security Platform or CECSP as a new regional cooperation. The regional agreement has created strategic and operational cooperation between the four Visegrád countries (the Czech Republic, Hungary, Poland, Slovakia), as well as Austria. The regional cooperation of the Central European countries is not a completely new initiative; there was another similar regional cooperation initiative like the CECSP, the so-called Central European Defence Cooperation (CEDC) established in 2011, aiming to facilitate the military-focused collaboration. Maybe the CECSP is the next step or the extension of the CEDC as all of the CECSP members are also members of the defence cooperation (Poland only as an observer). But it is important to highlight that the CEDC itself was not involved in the latter established CECSP cooperation, but as we will see later, the military cyber groups were also involved in it. There is only one similar, regional defence platform in

[1] Computer Security Incident Response Team.

[2] Computer Emergency Response Team.

Europe, NORDEFCO, founded by the Nordic countries, but it does not have a specific, cybersecurity-oriented agreement.[3]

The question may arise, considering that CECSP countries are participating in several already existing organisations, why do we need a regional cooperation, and what new role can be played by the CECSP in strategic or operational level cooperation. Is it possible to reach real operational cooperation or it is rather a strategic and diplomatic level regional cooperation?

To find the possible answers, I will give an overview on the cybersecurity policy of the platform's member states and their goals and activities in the cyberspace. I will present the history of the CECSP cooperation and its relations to the V4 cooperation and to the EU level regulation: *Directive on Security of Network and Information Systems* (NIS Directive). This study was prepared by using and updating an earlier case study: *Cybersecurity in the V4 Countries – A Cross-border Case Study.*[4]

The Cybersecurity Structure of CECSP Countries

Countries that are members of the platform participate in the cyberspace related work of the major international communities without exception. As the cybersecurity regulations of these communities are developing into the same direction and their members must implement these regulations, the CECSP countries have essentially similar legal and organisational structures.[5]

It is important to emphasise that before the *Directive on Security of Network and Information Systems* (NIS Directive) had been adopted in 2016, only guidelines and strategic objectives from international organisations and studies or guides about best practices showed examples internationally; therefore, the legal and organisational system of the countries was quite different.[6]

[3] Bence Németh: *Outside NATO and the EU. Sub-Regional Defence Co-Operation in Europe.* London, King's College, 2017.

[4] Anita Tikos – Csaba Krasznay: *Cybersecurity in the V4 Countries – A Cross-border Case Study.* Central and Eastern European e|Dem and e|Gov Days 2019. 163–174.

[5] Dániel Berzsenyi: Kiberbiztonsági analógiák és eltérések. A Közép-európai Kiberbiztonsági Platform részes országai által kiadott kiberbiztonsági stratégiák összehasonlító elemzése. *Nemzet és Biztonság,* 7, no. 6 (2014).

[6] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union.

To understand and clearly see the full picture about the regional cooperation, it is worth comparing the cybersecurity preparedness and system of the countries that are members of the platform based on their national strategy and organisation system. It will not be a detailed strategic and organisational analysis; the aim is only to highlight the main similarities and differences by drawing up a comprehensive picture.

The first national cybersecurity strategies were established at about the same time by the CECSP countries in the early 2010s. The Czech Republic was the first who published a national strategy on cybersecurity in 2008, then Slovakia in 2011, and finally Austria, Poland and Hungary, all in 2013.[7]

Of course, over the years these strategies have been reviewed, because the period of their effect has expired and/or the development of the technology brought new challenges to cover.

Therefore, Slovakia and the Czech Republic formulated their new second generational national strategy for the period 2015–2020, meanwhile Poland published its own in 2017.

After the NIS Directive was adopted, it became the obligatory model for all future strategy of every country. These principles do not have new strategic elements compared to the existing international practice, but this is the first time when these are not just optional elements of the national strategies.

Hungary found a special solution to comply with these requirements; as the strategy accepted in 2013 is a general one and the main aims are still valid, Hungary extended this cybersecurity strategy with the Network and Information Systems Security Strategy of Hungary in 2018, which is a "so-called" sectoral strategy.[8] As the title suggests, this sectoral strategy covers the main strategic requirements of the NIS Directive.

Poland decided to strengthen and develop systematically its national cybersecurity system while implementing the EU cybersecurity regulatory framework

[7] Government of Hungary: Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary. *ENISA,* 21 March 2013; Republic of Austria: *Austrian Cyber Security Strategy.* 10 March 2013; Government of Poland: National Framework of Cybersecurity Policy of the Republic of Poland. *ENISA,* 30 November 2017; Government of the Slovak Republic: Cyber Security Concept of the Slovak Republic. *ENISA,* 01 June 2015; Government of the Czech Republic: National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020. *ENISA,* 16 January 2015.

[8] Government of Hungary: Government Decision No. 1838/2018 (28 December 2018) on Hungary's Strategy for Network and Information Security.

(including the NIS Directive and Cyber Act); therefore, a new Cybersecurity Strategy of the Republic of Poland for 2019–2024 has been accepted.[9] The strategy of Slovakia and the Czech Republic was valid and has aims until 2020, so they published their third strategy in late 2020 and at the beginning of 2021.

The Czech Republic defined its new strategy for 2021–2025 in January 2021.[10] This strategy will continue to fulfil the vision of the previous strategy but with new solutions to the new threats. The most important aspect of the strategy is the resiliency and the capacities of state security services, state institutions, organisations and individuals. This strategy does not mention the NIS Directive, and does not define any definite regulatory or organisational process/requirement or change. The effective international cooperation is one of the aims of the strategy, and within this point the cooperation of the Central European region is also mentioned as one international cooperation platform where they plan to strengthen the country's active role. The resilient society 4.0 is one of the main aims of this strategy, where securing the digital society and public administration, education and awareness raising and expanding the qualified cybersecurity workforce are the main aims. On the other areas, the main aim is to strengthen the resilience, capacity building, preventing and fighting cybercrime, better information sharing and cooperation, define communication strategy and update its national regulations to be able to effectively react to new challenges, threats, etc.

The new Slovak strategy, the National Cyber Security Strategy 2021–2025 defined the strategic aims for the next five year. This strategy continues the concept and aims of the previous strategy, plus tries to address the new threats and challenges in a modern way to be able to respond to the constantly evolving cyber threats and cybersecurity, it defines the principles of the cybersecurity system to ensure a higher level of security in the cyberspace of the Slovak Republic. This strategy mentions the NIS Directive, but does not aim to implement it, as the implementation period has already expired. This strategy has several ambitious aims in the field of international cooperation (in different international organisations and in bilateral cooperation), but it does not mention the CECSP cooperation at all. Austria still does not publish a new strategy since 2013, or

[9] Republic of Poland: Uchwała Nr 125, Rady Ministrów w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024. 12 October 2019.

[10] National Cyber Security Center (NCKB): National Cyber Security Strategy of the Czech Republic for the Period from 2021 to 2025. *NUKIB,* 18 March 2021.

any assessment about the compliance of the strategy with the requirements of the NIS Directive and the new threats and challenges within the cyberspace.

We can say that all national strategies (every generation) of all five countries include the relevant areas from international (ENISA, NATO, ITU) cybersecurity strategy guidance, such as objectives for education, research and development, awareness-raising, public–private partnership, law enforcement, international cooperation and critical infrastructure protection.

In case of the first and second generational strategies, they vary from the legislative perspective. Some of the strategies aims at the creation or the update of a comprehensive information security regulation (in case of Slovakia or Poland), while for other countries they refer specifically to the legal regulation of one or two areas in the strategy paper (for example in the case of Hungary).

Regarding cybersecurity organisations, it must be highlighted that all evaluated strategies identify the governmental and/or national incident management centre (GovCERT/national CERT), the regulatory body with rights and responsibilities and the organisation or ministry responsible for coordination and for decision-making.[11]

There is a discrepancy between the strategies – in the first two generations – regarding the non-governmental areas (for example: regarding the critical infrastructure sectors), and in the organisational coverage. The other difference is that the development of regulations and the creation of specialised organisations can be observed only as a goal in some sectors, while in other cases the critical infrastructure and/or sectoral regulations are already existing, and the goal is to strengthen and further develop them.

Each evaluated strategy deals with the question of non-governmental, sectoral CERTs and the establishment of military CERTs. The countries have a same approach in terms of the need for the creation of special sectoral CERTs, but they are in different stages in the implementation. In Austria, there are many commercial CERTs operating and the country has a military CERT (MilCERT), whereas in Hungary and the Czech Republic one of the objectives is the establishment of a sectoral CERT.

Each strategy highlights the importance of the active international cooperation, mainly referring to the European Union and NATO, but in several cases the regional cooperation (or especially the Central European cooperation) has been highlighted as a priority.

[11] Lászó Kovács: *Kiberbiztonság és -stratégia.* Budapest, Dialóg Campus, 2018.

Regarding the third generational strategies, we can say that they cover the same main elements, sectors and institutional requirements but they still vary in detail (regarding their priorisation and the chosen legal and organisational solutions in detail). In the Hungarian sectoral strategy, one important aim is to strengthen the international and regional cooperation.

In the new Polish, and Czech strategy, the active international cooperation at the strategic and political level is also an important aim, where the Central European cooperation is also mentioned as an important cooperation platform, but the new Slovak strategy does not have any aim or reference to the CECSP at all.

It is important to know that the strategies cannot be used to draw a conclusion on the similarity or differences of the organisational structures, as a number of organisational development and transformation took place in the countries during the adoption of their strategies, that cannot be read out directly from the strategy itself, such as the creation of commercial CERTs or the military CERTs. For example, in Hungary the organisational structure has changed several times, and the main changes in the last 5 years (for example: in 2015, the National Cyber Security Center, so-called NCSC was set up by uniting 3 existing cybersecurity related organisations, or the Defense Sector Electronic Information Security Incident Management Center – MilCERT was established on 1 March 2016) was also not covered directly by the national cyber strategy but still supports the implementation of the strategic aim to create the necessary specialised cybersecurity related institutions:

In conclusion, the national strategies have shown us that the CECSP countries have similar priorities and timelines at strategic level, and the international and regional cooperation is an important aspect for every country since the beginning.

The Historical Background and the Main Aims of the Central European Cyber Security Platform

In accordance with the fundamental objectives of the CECSP countries, the main aims of the thematic regional cooperation are to work together in accordance with the guidelines and initiatives of the EU and NATO and to support each other with their experiences in developing a national cybersecurity legislation and organisational structure. The most important goal of the platform is to gain more defence and resiliency in case of cyberattacks through this regional cooperation.

The idea of setting up this regional platform can be originated from the historical foundations of the Visegrád countries, which are resting on a cooperative approach since 1991. The Visegrád cooperation is based on the main common aims of the countries concerned like geographical relations, historical traditions, the Euro-Atlantic security system and the accession to the Euro-Atlantic organisations.

20 years later, when the CECSP cooperation was created, the original aims of the Visegrád cooperation was already achieved, but the cooperation was still preserved, to support each other in development and to be able to assert their interest in the international communities. Therefore, the original political Visegrád cooperation has been supplemented with independently operating thematic cooperation like the CEDC and CECSP.

The Central European cybersecurity cooperation is a comprehensive approach to cybersecurity issues, covering major levels of cybersecurity (strategic–operative, government–military, national–international). Accordingly, representatives of the platform include the ministries responsible for cybersecurity, military and national CSIRTs and authorities responsible for information security. In addition, the European Network and Information Security Agency (ENISA) has an observer position in the platform to support the aims and work of the platform with its international experience.[12]

In CECSP, the most important strategic aim of the members is to be more successful in international, community (EU) or allied (NATO) lobbying and to be able to represent a regionally discussed and agreed single position. As a result, Member States will have an opportunity to better reach out the consideration and validation of their positions and proposals on community or allied level. This also can be an important element of cyber diplomacy, to be able to assert our position by getting support from our regional partners. Such cooperation has been observed over the past years during the negotiation of cybersecurity regulations within the European Union (such as the NIS Directive or the EU Cybersecurity Act).

After the establishment of a common, European level international regulation (for example, the adoption of the NIS Directive), the support function of the platform is still important for all of the members, as it can also provide a podium

[12] European Union Agency for Network and Information Security: Meeting of the Central European Cyber Security Platform 2014. *ENISA News,* 10 April 2014.

for discussing legal and technical questions arising during the implementation and evaluating cooperation mechanisms.

Another objective of this cooperation at the strategic level is to create a platform between the countries to support cooperation and share experience in R&D projects, but in practice, there was no visible cooperation or even information sharing within (or with the support of) the platform about their experiences in R&D projects. Probably the regulatory questions were bigger priority or R&D is still such a sensitive topic that it is more important than information sharing and cooperation.

At the beginning, the establishment of cooperation on the operational level was also a huge priority, which is realised in the CERTs/CSIRTs cooperation. As it was seen in the strategies, the objective of most countries was to set up different CSIRTs or to develop the existing ones; information sharing and learning from the experiences of others are essential for the CSIRTs. Just like in other CSIRT communities, members share their experiences, report lessons learnt of major successful or failed attacks and good practices to community members, and make their collaboration more effective by organising cybersecurity exercises in order to develop the skills and preparedness of IT security professionals for current cybersecurity challenges and attacks.

At the beginning, the most important elements on the agenda of the Platform was the CSIRT cooperation (and practice the possible cooperation forms by cyber exercises) and to present and explain to each other their regulatory and organisational framework.

The Operational Model of the CECSP

In 2013, during the establishment of the Platform, the main goal was to build trust, to define a cooperation framework and its rules. After all, there was a need to develop a work program also for the platform.

According to the defined rules, the Platform has at least one strategic and operational meeting each year. The members decided to set up a presidency model, where the presidency is responsible for the management of the platform and the organisation of the meetings. Member States fill the presidency in a rotating system for one year (in alphabetical order). Hungary acted as chairman of the platform in 2015, and in 2020 also Hungary had the chairman position and responsibility.

During the first Hungarian platform presidency in 2015, there was a strategic decision-makers working group meeting and an operational level meeting in Budapest.

Unfortunately, the official work programs of the CECSP presidencies are not publicly available, but we could identify the main aims and most important tasks of the presidency periods thanks to the published Presidency summaries after the events, and to the references to the CECSP's aims and activities in the V4 presidency programs.

In the first few years, the platform organised various cybersecurity exercises for its members yearly, despite the fact that all participating national CERTs in the platform are taking part in EU and NATO exercises. Involving cybersecurity professionals in red and blue teaming exercise can also provide an opportunity to test and discuss the experiences gained in the allied and community exercises.

Until now, Hungary has organised two exercises for the members of the platform. The first one was held on 23 June 2014, right after the establishment of CECSP.[13] The second one was a decision-making and procedural exercise (Table Top Exercise, TTX) in 2015, during the Hungarian presidency period of the platform. The latest exercise took place in May 2017 in Brno, the Czech Republic. It was developed by the Masaryk University and was held in a special environment. This exercise did not focus on cooperation, but on testing and developing the technical skills of participating players.[14] In 2018, no regional exercise took place, as all countries participated at the ENISA's Cyber Europe 2018 cyber crisis exercise event.

Cybersecurity on the Political Level in V4 Cooperation

As it was mentioned and explained before, CECSP is independent from the Institutional Visegrád 4 cooperation and from the Central European Defence Cooperation (CEDC) either, but it could not have taken place without the political support of the governments of the concerned countries. As soon as the political leaders realised the potential impact of cyberattacks, the need of cyber defence on regional level has appeared in the presidency programs (with respect to the

[13] Ádám Draveczki-Ury: Szoros együttműködés a kibertérben. *Honvedelem.hu,* 27 June 2014.

[14] National Cyber Security Center (NCKB): *National Cyber Security Centre Held Exercise for CECSP Partners.* 24 May 2017.

CECSP work program itself) and has evolved parallelly with the NATO–EU objectives.

Naturally, the higher politically represented V4 cooperation has influence and/or refer to the CECSP aims and work program; therefore, it is important to collect and see the cyber-related goals of each V4 presidency from 2012, where this issue was first mentioned.

2012–2013 Polish Presidency

Cybersecurity was first mentioned in the Visegrád 4 work program in a military context:

> "There will be a need for V4 consultations on NATO–Russian relations, a V4 common position on Missile Defence and on the Russian response, on NATO cooperation with Ukraine and Georgia, consultations on CFE and force deployment in the region, consultations, in the broader format of V4+ Baltic states + Romania and Bulgaria, on common security issues, and with regard to cyber security and energy security."[15]

2013–2014 Hungarian Presidency

In this year, cybersecurity got a higher focus because of the establishment of the CECSP, and there was already technical meetings as well, led by the Czech Republic.[16] The V4 members described their goals on political level as follows:

> "– Emphasizing the importance of cyber security awareness and strengthening dialogue and cooperation at policy and operational level in the field of cyber defense;
> – Promoting efforts to make information exchange and knowledge transfer (lessons learned and best practices) more efficient in the field of cyber and information security.
> – Exchange of knowledge and practical expertise countering cybercrime with Western Balkan countries."

The military approach can also be found in this presidency program, as well as cybercrime and cyber diplomacy. The "concrete proposals for discussion" of the

[15] Ministry of Foreign Affairs of the Republic of Poland: Programme of the Polish Presidency of the Visegrad Group. *International Visegrad Fund,* 1 July 2012.
[16] CSIRT.CZ: *Zástupci CSIRT.CZ se zúčastnili setkání platformy CECSP.* 28 December 2013.

V4 countries "include the setting up of a long-term cyber security cooperation mechanism" in the context of security policy related to NATO and the Common Security and Defence Policy of the European Union. They also "endeavour to strengthen the V4–B3 cooperation, particularly in the fields of […] cyber security" and promote further cooperation with the Western Balkan countries "on judicial cooperation in criminal matters and fight against corruption, and fight against cybercrime".[17]

2014–2015 Slovak Presidency

Information and cybersecurity got a separate chapter in this presidency program and became one of the major issues. "The primary objective is to increase the immunity of information systems in the V4 countries against cyber-attacks and to decrease computer-based crime." To reach this goal, the Slovak presidency focused on the following topics:

> "– Streamlining management of information/cyber security, security risk management;
> – Protecting human rights and fundamental freedoms in connection with the use of information and communication infrastructure (including the Internet);
> – Increasing awareness and competencies, education in the area of information/cyber security;
> – Cooperation at international level in the area of information/cyber security (exchanging skills, experience and sharing information);
> – Completing mutual consultations in order to harmonize the approaches taken by V4 countries and considering mutual support when adopting decisions and their subsequent implementation within international organizations (EU, NATO, UN and others);
> – Supporting an improvement in the standing of the Central European Cyber Security Platform;
> – Creating a safe environment (prevention, response to security incidents, the scope of specialized CSIRT/CERT-type teams, for example the implementation of joint simulation exercises on critical information infrastructure protection, creating a secure communication channel to share information on current threats and on-going large-scale security incidents, linking of early warning and information sharing in the V4."[18]

[17] Ministry of Foreign Affairs and Trade of Hungary: Hungarian Presidency in the Visegrad Group (2013–2014). *International Visegrad Group,* 1 July 2013.

[18] Ministry of Foreign and European Affairs of the Slovak Republic: Programme of the Slovak Presidency of the Visegrad Group, July 2014 – June 2015. *International Visegrad Group,* 1 July 2014.

This program has defined the scope of CECSP cooperation, and the platform is still working according to the above described principles. In this year, cyber did not appear in any other relation, except the defence and security policy part, where it was treated as a general security risk.

2015–2016 Czech Presidency

The Czech Presidency placed cybersecurity to the operational level. As CECSP's operational capability has been proven, this issue disappeared from the list of strategic questions. The Presidency Program has the following statement:

> "Cybersecurity is also a prospective topic for the Visegrád cooperation. The CZ V4 PRES will push to deepen and increase the efficiency of cooperation within the Central European Cyber Security Platform (CECSP). This will particularly include harmonising the positions of the V4 countries on fundamental topics of cyber security, including their positions within international organisations, organising expert workshops and introducing standards and secured channels as part of communication among the CECSP states. The V4 will also continue in the practice of cooperation among specialised police units and national 'centres of excellence' focused on research in the area of cybernetic crime."[19]

The Czech National Security Authority got the task to facilitate the operational level cooperation. For this, their planned activities also were specified in the program:

> "– At the strategic level, the CZ V4 PRES will seek progress in harmonising the approach of individual states and their positions and opinions on major cyber security issues within international organisations, forums and discussions. This includes primarily the legislation being negotiated in the working bodies of the Council of the EU and European Commission and documents negotiated under the OSCE and International Telecommunication Union;
> – At the operational level among top CERT sites, we want to organise workshops on selected topics (e.g. intrusion detection and honeypots, penetration testing, etc.);
> – The CZ V4 PRES is committed to implementing standards and secure channels in communications among CECSP states."[20]

[19] Ministry of Foreign Affairs of the Czech Republic: Programme for the Czech Presidency of the Visegrad Group 2015–2016. *International Visegrad Fund,* 1 July 2015. 12–29.
[20] Ibid.

2016–2017 Polish Presidency

Following the approach of the previous year, cybersecurity remained on the technical level and highlights the importance of CECSP. This area is summarised only in one paragraph:

> "Cyber-security: cooperation to enhance the protection against cyber threats inter alia by means of CSIRT cooperation and the Central European Cyber Security Platform (CECSP); building permanent relations between the CECSP and the V4. Furthermore, encouraging cooperation between special Police units and national 'centres of excellence' that focus on conducting research in the field of cyber-crime."[21]

Cybersecurity also disappeared from the defence policy and was only mentioned once under the police cooperation part, in relation with cybercrime. Probably the reason behind this reduced priority can be found in the European legislation. As, in this period, the NIS Directive was adopted and required a pan-European approach for cyber defence. The need for a regional cooperation has seemingly decreased.

2017–2018 Hungarian Presidency

2017 was a turning point in the era of cybersecurity. There were two state sponsored malware campaigns (WannaCry and NotPetya) that caused global chaos, meanwhile more and more details had been revealed on the effects of cyber-attacks during the U.S. presidential election. The Hungarian Presidency Program clearly reflects to these threats and cyber defence got a higher focus than in the previous year.

First of all, due to hybrid threats, cybersecurity is mentioned in a military context again:

> "Defence policy cooperation in the V4 + Ukraine and V4 + Moldova formats, focusing on examining possibilities for joint work on defence sector reform, sharing experience on cyber defence and hybrid war, resilience and a potential involvement in the V4 EU Battlegroup (in the case of Ukraine)."

[21] Ministry of Foreign Affairs of the Republic of Poland: Programme of the Polish Presidency of the Visegrad Group 2016–2017. *International Visegrad Fund,* 1 July 2016. 14.

This is emphasised with a planned Cyber Workshop between the V4 countries and the United States.

On the other hand, the operational cooperation is described in more details:

> "In the field of cyber security, the Presidency's goal is to strengthen the resilience of critical infrastructure, especially with the aim of revealing and averting risks and attacks coming from the cyberspace. The Hungarian Presidency will carry on the cooperation between cyber security organisations and network security centres of V4 countries, for which information-sharing on incidents is indispensable. In cooperation with the rotating Chair of the Central European Cyber Security Platform, the Hungarian Presidency will organise expert meetings and joint exercises and trainings related to incident management. The Presidency also plans to hold consultations aiming to formulate joint V4 positions on current topics of the EU's agenda, in particular on the implementation of the Directive on Security of Network and Information Systems (NIS Directive), and the revision of the Cybersecurity Strategy of the EU."[22]

2018–2019 Slovak Presidency

This Presidency Program also deals with cybersecurity, but it is not as ambitious as it was in the previous year. It focuses on cybercrime and the usage of cryptocurrencies:

> "Digital evolution and the development of cyber space bring an increasing number of cyberattacks, which, in some EU Member States, even exceed the number of standard crimes. Therefore, within the Presidency of the V4, we shall focus on the strengthening and improvement of cooperation in the fight against cybercrime connected with the misuse of crypto currencies, especially bitcoin."

Then it turns to CECSP and highlights the success of the Slovak Presidency of this forum in 2017:

> "With regard to CECSP cooperation, during the Slovak Presidency in 2017 the member countries started to coordinate their activities, stances, and positions even on the EU level. This initiative did not go unnoticed by other members of the EU. For example, as a result France joined in on the coordination of CECSP activities in matters of the cybersecurity of the European Union."[23]

[22] Ministry of Foreign Affairs and Trade of Hungary: Hungarian Presidency 2017–2018 of the Visegrad Group. *International Visegrad Group,* 1 July 2017. 15–16.

[23] Ministry of Foreign and European Affairs of the Slovak Republic: Dynamic Visegrad for Europe, Slovak Presidency 2018–2019 of the Visegrad Group. *International Visegrad Group,* 1 July 2018. 18.

2019–2020 Czech Presidency

This presidency program is also not too ambitious regarding cybersecurity as it is nearly just mentioned in the detailed presidency program.

The Czech presidency program has 3 main priority areas (mentioned as a 3R), and cybersecurity related topics are covered in the second one. This area is the area of the Revolutionary technologies, where presidency aims to deal with

> "innovative economy and its social impacts: CZV4PRES will concentrate on support for research, development and innovation, innovative ecosystem, Digital Single Market, artificial intelligence but also on education and adaptability of people to the related changes in the labour market."[24]

As part of the detailed presidency program, the Czech presidency mentions cybersecurity-related topics also as part of the security policy

> "to include European defence initiatives and the development of the civilian component of the Common Security and Defence Policy. The objective is to enhance security and defence cooperation especially in collective defence, military mobility, cyber security, hybrid threats, terrorism, strategic communication capabilities, and regarding challenges emanating from the South."

Cybercrime and critical infrastructure protection is also mentioned in the presidency program, with the aim to

> "promote closer V4 exchange of experience and cooperation on cybercrime, especially between national cybercrime contact points and law enforcement authorities (public prosecutors and the police). The focus should be on the protection of critical information infrastructure and important information systems."[25]

Supporting these goals, only one event, a conference has been organised (and planned in the work program) in November 2019, by the Czech Republic Police about the current trends in cybercrime and cybersecurity.

[24] Ministry of Foreign Affairs of the Czech Republic: *The Czech Republic Holds the Presidency of the Visegrad Group from 1 July 2019 to 30 June 2020.* 25 June 2019.

[25] Ministry of Foreign Affairs of the Czech Republic: Programme for the Czech Presidency of the Visegrad Group 2019–2020. *Visegrad Group,* 06 September 2019.

In this presidency program, the CECSP cooperation or the operational cybersecurity cooperation has not been mentioned, furthermore the work program defines task and cooperation only for the police and for the Ministries of Foreign Affairs.

Probably the reason of the disappearance of the CECSP and operational cyber policy from the V4 presidency programs could be found in the developed EU cyber policy. For this time, this cooperation forms were established in EU level by the NIS Directive and Cyber Act, and the possible future work must be raised within the parties in the future.

2020–2021 Polish Presidency

The pandemic situation and its consequences have a huge effect on the presidency program of 2020–2021; therefore, the Polish presidency will mainly focus on the Covid-related issues, but cybersecurity can also be found in its agenda, as an important issue in a pandemic situation like the Covid-19.

The Polish residency is planning to discuss its initiatives in the cybersecurity area:

> "Signing a joint declaration on mutual cooperation in cyber security, to serve as a roadmap for V4 activities – main activity areas include:
> – increasing the capability for reacting to incidents by, among others, developing the management of cross-border incidents in combination with consultations, as well as conducting international exercises to improve adaptation in taxonomy, collection and analysis of digital evidence and collaboration in prosecuting cyber criminals;
> – building common situational awareness in cyber space, especially by exchanging information on cyber threats in real time between national level CSIRT teams;
> – developing new methods and tools to test, assess and certify ICT products, processes and services (as part of the Cyber Security Act);
> – developing a new generation of cryptographic algorithms resistant to quantum computing;
> – improving multilateral collaboration and national capabilities in cyber security, among others in the R&D area."[26]

Furthermore, the Polish presidency is planning to consult within the CECSP platform about the other possible topics (like cross-border incident handling;

[26] Ministry of Foreign Affairs of the Republic of Poland: Presidency Programme of Polish Presidency of the Visegrad Group 2020–2021. *International Visegrad Fund,* 1 July 2020.

situational awareness; R&D, supply chain security; digital evidence and international law applicable to cyberspace operations) that can be involved within the regional cooperation.

Efficiency, Benefits and Future of CECSP Cooperation

As we saw before, the participating countries have common objectives, basic regulations and an organisational system for the operation of the Central European Platform. Since the establishment of the cooperation, mainly operational and strategic discussions and cybersecurity exercises were on their agenda. The essential and basic requirement for the effective functioning of the cooperation is to build trust between the parties involved in the agreement. We can say that the countries participating in the platform are familiar with the legal and organisational specialties of each other in detail and had the opportunity to build up trust and to understand other parties. This completely meets our definition of cyber diplomacy.

As a result, they had opportunity for detailed technical consultations, discussions and could identify additional actors and areas of expertise for the further development and deepening of the cooperation.

After examining the work programs of the platform, we could see that this cooperation mainly stayed at the strategic cooperation level, where political (EU, NATO and national) legal and diplomatic questions have been discussed. We also saw some intention for a deeper cooperation by involving CSIRTs in this cooperation, but it stayed on a higher level by sharing best practices, introducing themselves and their main knowledge (but not in detail). Cyber exercises do not mean real cooperation either; it is just practicing their ability and cooperation model. IT helps to build trust, but it is still far from real life technical cooperation (in case of an incident, or a project etc.).

As it was mentioned above, the NIS Directive, adopted in 2016, is the first European regulation to provide mandatory legislative and technical (CSIRT) cooperation and defines minimum requirements in the national regulation for the Member States. Accordingly, the CECSP Member States had to review their national cybersecurity strategy, in line with NIS requirements, as well as their national legislation for the core services sectors and the sectors providing digital services. As a result, the CECSP member states have the same national strategy, national regulations and organisational structure and are set up on the same basis.

Thanks to the directive, collaboration and information sharing between CSIRTs is implemented through binding rules, in case of incident reporting and cross-border incident management as well. The technical training and testing area are also covered by the European Union regulations, as there are mandatory exercises, like the Cyber Europe exercise in every two years, and the exercises of the CSIRTs Network.

The question may arise that after these rules and cooperation mechanisms established by the NIS Directive, what can be the role of the CECSP regional cooperation if all its countries are members of the EU and must apply the EU level cooperation.

It is undeniable that the strategic and technical cooperation elements of the Platform are covered by the new EU rules, and the V4 presidency programs and the decrease of the operation of the CECSP meetings also pointing to the direction that CECSP has been replaced by the EU level cooperation.

On the other hand, most of the members still mention the need and the importance of the regional cooperation in their new cybersecurity strategies, so probably they do not plan to terminate the platform, but they have their main focus on other international cooperation.

Maybe it would be important to find new aims and cooperation areas for the platform, as the active cooperation and effectiveness of the platform decreased since the implementation of the NIS Directive.

2020 seemed to be an interesting and promising year from several perspectives: first of all, Hungary held the presidency of the platform again, and that could have been a huge opportunity to discuss and refresh the aims of the platform. Secondly, in 2020 the European Commission assessed the implementation and effectiveness of the NIS Directive and defined the suggestion on how to redraft the directive, and it could also have been a good opportunity to draft a common position and suggestion for the Commission about the NIS Directive. Unfortunately, in that year the Covid crisis has overwritten every kind of plans, events and discussions, and maybe it has a negative effect on such regional policy-related discussions as well. Unfortunately, we do not have any publicly available information or report about the programme or results of the 2020 programme of the platform, but probably the programme has been minimised to discuss the Covid-related issues, and the NIS-related review, and probably the events must be delayed or changed to remote events, which also reduces the effectiveness of such discussions.

But there are several promising issues that could be discussed, and handled within the platform, as they are still not regulated by the EU, and it could add

value to the regional work. The participants can review the existing CECSP cooperation and involve more professionals from other areas, and extend the cooperation with some other, more specialised areas (such as research and development, education, awareness raising, law, professional training, common EU research applications, cross-sectoral issues, etc.). The support of actual CECSP parties (ministries, authorities and CSIRTs) for the new areas of the regional cooperation could help the new partners in trust- and confidence-building and could be a good basis to start a valuable, deep and daily cooperation.

Finally, it should be emphasised that the platform still gives a good opportunity for its members to develop a stronger common position on international level and can be a forum to discuss ideas, questions and experiences at the transposition stage as they have already done regarding the NIS Directive and the Cybersecurity Act.

As we can see, cyber diplomacy is an important and integral element of the regional cooperation of the Visegrád countries, were they have an opportunity to discuss legal and organisational (and maybe technical) questions, as well as questions of cooperation, to develop together different cyber exercises to have an opportunity to establish a common position to be able to validate their position in other international forums.

References

Berzsenyi, Dániel: Kiberbiztonsági analógiák és eltérések. A Közép-európai Kiberbiztonsági Platform részes országai által kiadott kiberbiztonsági stratégiák összehasonlító elemzése. *Nemzet és Biztonság,* 7, no. 6 (2014). 110–136.

CSIRT.CZ: *Zástupci CSIRT.CZ se zúčastnili setkání platformy CECSP.* 28 December 2013. Online: www.csirt.cz/page/1836/zastupci-csirt.cz-sezucastnili-setkani-platformy-cecsp/

CSIRT.SK: *Third meeting of CECSP: Tretie rokovanie Stredoeurópskej platform kybernetickej bezpečnosti.* 11 April 2014. Online: www.csirt.gov.sk/aktualne-7d7.html?id=69

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148

Draveczki-Ury, Ádám: Szoros együttműködés a kibertérben. Honvedelem.hu, 27 June 2014. Online: https://honvedelem.hu/cikk/szoros-egyuttmukodes-a-kiberterben/

European Union Agency for Network and Information Security: Meeting of the Central European Cyber Security Platform 2014. *ENISA News,* 10 April 2014. Online: www.enisa.europa.eu/news/enisa-news/central-european-cyber-security-platform-2014

Federal Ministry for Digital and Economic Affairs: Central European Cyber Security Platform. *Digitales Österreich,* 11 April 2014. Online: www.digitales.oesterreich.gv.at/-/central-europeancyber-security-platform

Government of the Czech Republic: National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020. *ENISA,* 16 January 2015. Online: www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

Government of Hungary: Government Decision No. 1838/2018 (28 December 2018) on Hungary's Strategy for Network and Information Security.

Government of Hungary: Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary. *ENISA,* 21 March 2013. Online: www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf

Government of Poland: National Framework of Cybersecurity Policy of the Republic of Poland. *ENISA,* 30 November 2017. Online: www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/govermental-program-for-protection-of-cyberspace-for-the-years-2011-2016-2013

Government of the Slovak Republic: Cyber Security Concept of the Slovak Republic. *ENISA,* 01 June 2015. Online: www.enisa.europa.eu/topics/national-cyber-securitystrategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1

Kovács, László: *Kiberbiztonság és -stratégia.* Budapest, Dialóg Campus, 2018.

Ministry of Foreign and European Affairs of the Slovak Republic: Programme of the Slovak Presidency of the Visegrad Group, July 2014 – June 2015. *International Visegrad Group,* 1 July 2014. Online: www.visegradgroup.eu/documents/presidencyprograms/sk-v4-pres-program-2014

Ministry of Foreign and European Affairs of the Slovak Republic: Dynamic Visegrad for Europe, Slovak Presidency 2018–2019 of the Visegrad Group. *International Visegrad Group,* 1 July 2018. Online: www.visegradgroup.eu/documents/presidency-programs/slovak-v4-presidency-en

Ministry of Foreign Affairs and Trade of Hungary: Hungarian Presidency in the Visegrad Group (2013–2014). *International Visegrad Group,* 1 July 2013. Online: www.visegradgroup.eu/documents/presidency-programs/hu-v4-presidency-2013

Ministry of Foreign Affairs and Trade of Hungary: Hungarian Presidency 2017–2018 of the Visegrad Group. *International Visegrad Group,* 1 July 2017. Online: www.visegradgroup.eu/documents/presidency-programs/hungarian-v4-presidency

Ministry of Foreign Affairs of the Czech Republic: Programme for the Czech Presidency of the Visegrad Group 2015–2016. *International Visegrad Fund,* 1 July 2015. Online: www.visegradgroup.eu/documents/presidency-programs/cz-v4-pres-2015-2016

Ministry of Foreign Affairs of the Czech Republic: *The Czech Republic Holds the Presidency of the Visegrad Group from 1 July 2019 to 30 June 2020.* 25 June 2019. Online: www.mzv.cz/jnp/en/foreign_relations/visegrad_group/index.html

Ministry of Foreign Affairs of the Czech Republic: Programme for the Czech Presidency of the Visegrad Group 2019–2020. *Visegrad Group,* 06 September 2019. Online: www.mzv.cz/file/3626458/Programme_CZ_V4_PRES_2019_2020_A.pdf

Ministry of Foreign Affairs of the Republic of Poland: Programme of the Polish Presidency of the Visegrad Group. *International Visegrad Fund,* 1 July 2012. Online: www.visegradgroup.eu/documents/presidency-programs/programme-of-the-polish

Ministry of Foreign Affairs of the Republic of Poland: Programme of the Polish Presidency of the Visegrad Group 2016–2017. *International Visegrad Fund,* 1 July 2016. Online: www.visegradgroup.eu/documents/presidency-programs/pl-v4-pres-2016-17

Ministry of Foreign Affairs of the Republic of Poland: Presidency Programme of the Polish Presidency of the Visegrad Group 2020–2021. *International Visegrad Fund,* 1 July 2020. Online: www.visegradgroup.eu/documents/presidency-programs/2020-2021-polish

National Cyber Security Center (NCKB): *Central European Cyber Security Platform 2014.* Online: www.govcert.cz/cs/informacni-servis/akce-udalosti/2140-central-european-cyber-security-platform-2014/

National Cyber Security Center (NCKB): *National Cyber Security Centre Held Exercise for CECSP Partners.* 24 May 2017. Online: www.govcert.cz/en/info/events/2532-national-cyber-security-centre-held-exercise-for-cecsp-partners/

National Cyber Security Center (NCKB): National Cyber Security Strategy of the Czech Republic for the Period from 2021 to 2025. *NUKIB,* 18 March 2021. Online: www.nukib.cz/download/publications_en/strategy_action_plan/NSCS_2021_2025_ENG.pdfNational

Security Authority (NBU): The National Cybersecurity Strategy 2021–2025. *NBU,* 07 January 2021. Online: www.nbu.gov.sk/wp-content/uploads/cyber-security/National_cybersecurity_strategy_2021.pdf

Nemzeti Kibervédelmi Intézet: Megrendezésre került a Közép-európai Kiberbiztonsági Platform (CECSP) konferencia. *NKI,* 21 December 2013. Online: https://nki.gov.hu/figyelmeztetesek/archivum/megrendezesre-kerult-a-kozep-europai-kiberbiztonsagi-platform-cecsp-konferencia/

Németh, Bence: *Outside NATO and the EU. Sub-Regional Defence Co-Operation in Europe.* London, King's College, 2017. Online: https://kclpure.kcl.ac.uk/portal/files/80807208/2017_Nemeth_Bence_1212105_ethesis.pdf

Republic of Austria: *Austrian Cyber Security Strategy.* 10 March 2013. Online: www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf

Republic of Poland: Uchwała Nr 125, Rady Ministrów w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024. 12 October 2019. Online: http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

Tikos, Anita – Csaba Krasznay: *Cybersecurity in the V4 Countries – A Cross-border Case Study.* Central and Eastern European e|Dem and e|Gov Days 2019. 163–174. Online: https://doi.org/10.24989/ocg.v335.13

The purpose of the volume is to provide the reader with the key tools needed to navigate the realm of cyber diplomacy. It is not exhaustive in detailing all aspects of cyber diplomacy; instead, our work highlights the key pillars needed to understand a varied and complex topic from a European viewpoint. Balázs Mártonffy provides an overview of the key terms and relevant literature of the topic. Anna Molnár offers an introduction to the strategic and institutional framework of the EU's cybersecurity policy. Dóra Molnár demonstrates how European traditional diplomatic powerhouses fare in the realm of cyber diplomacy. Dóra Dévai focuses on the institutionalisation of the cyberspace policy of the European Union, and accounts how the EU's cyberspace policy evolved. Csaba Krasznay provides an overview of the "WannaCry" and the "NotPetya" attacks, and details the Western response. Anita Tikos focuses on the roles and efforts of the Visegrád Four states in cyber diplomacy, highlighting the importance of the group's rotating presidency.

ISBN 978-963-531-827-8
9 789635 318278