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come as no surprise that any text on an issue as complicated and quickly changing as the cyber domain is bound to be outdated quickly.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.

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.