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come as no surprise that any text on an issue as complicated and quickly changing as the cyber domain is bound to be outdated quickly.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