Winter 12-13-2018

Mitigating Cyber Warfare through Deterrence and Diplomacy

Annika Heffter
University at Albany

Sanjay Goel
University at Albany

Mitigating Cyber Warfare through Deterrence and Diplomacy

Annika Heffter[1]
University at Albany
Albany, New York, USA

Sanjay Goel
University at Albany
Albany, New York, USA

ABSTRACT

Nation states are increasingly bolstering their defensive and offensive cyber capabilities to launch and deter politically motivated cyber attacks. This does not only affect political processes, institutions, and election outcomes, but also a state's critical infrastructure, economy, and society. Recent escalations and cyber attacks on power grids, parliaments, electoral campaigns, and financial institutions have made governments more aware of the double-edged sword presented by emerging cyber capabilities wielded by nation states. A new layer has been added to conflict prevention between states, i.e. international diplomacy, confidence-building measures and deterrence in cyber space. In this paper, we argue that stand-alone deterrence and stand-alone appeasement cannot solve the arising cross-national cyber conflict and prevent a cyber arms race. Only a concerted effort to combine diplomatic and deterring strategies can lead to an acceptable status quo in international cyber relations.

Keywords: Cyber Diplomacy; Cyber Deterrence; Conflict Prevention; International Cyber Relations; Cyber Warfare; CBMs.

INTRODUCTION

The world faces an escalating threat from cyber weapons, which are becoming increasingly potent corresponding with our growing dependence on cyber infrastructure. Modern

[1] Corresponding author. annika.heffter@gmx.de +49 160 91021879

technological advances, enabled by cyber innovations, have impacted every facet of life, to the degree that governments, individuals and businesses depend on the digital world for day-to-day functions. Simultaneously, the threat landscape has broadened with each cyber innovation, and the consequences of attacks have escalated from information loss, to financial loss, to loss of life and property. Nation states have recognized the potential of cyber attacks for military use and are actively developing their digital arsenals, which could lead to a cyber arms race. The result of such an arms race would negate the economic and social gains of cyber space. There is a need for a combined, comprehensive approach of international diplomacy and deterrence to mitigate the cyber arms race before it leads to a catastrophic incident.

The development of sophisticated cyber weapons disrupts the implementation of traditional approaches to avert conflict and to prevent attacks. During the Cold War, deterrence first became a major theoretical concept to rational decision-making in tense political situations and in relation to cost-benefit calculations. However, historically, deterrence theory was not the only focus of the players in the international arena – diplomacy, open and secret negotiations and confidence-building measures (CBMs) helped to keep the balance of power when dissuasion and deterrence either did not work, or when diplomacy was needed in addition to deterrence. Both the conception and deployment of cyber deterrence strategies and confidence-building measures has become more difficult, for a number of reasons: (1) Cyber attacks and exploits are relatively cheap and can have significant impact, (2) Due to secrecy and a lack of transparency in the cyber domain, nation states do not disclose their capabilities, making it harder to deter adversaries or to cooperate with one another, and (3) Attributing cyber attacks with overwhelming confidence is almost impossible. Hence, political processes and institutions, economies and populations are at risk of being influenced and compromised by adversaries.

This paper examines the deterrence of nation states, and the diplomatic efforts between nation states. While outlining the challenges and advantages of transferring deterrence theory and confidence-building measures to the cyber realm, this paper mainly aims at elaborating on the intertwined nature of both approaches. Deterrence does not work without diplomatic effort, trust and credibility, and cooperative advances towards political and strategic adversaries do not yield positive long-term results without defensive and dissuasive strategies in place. Therefore, a more comprehensive approach is necessary to prevent conflict in cyberspace.

In order to understand the connection between deterrence theory and international diplomacy, we first lay out the key elements of cyber diplomacy and cyber deterrence. The subsequent discussion addresses the challenges and opportunities in combining cyber diplomacy and cyber deterrence to more effectively prevent politically motivated attacks.

INTERNATIONAL CYBER DIPLOMACY

International diplomacy and confidence-building measures in cyberspace still fall short of effective implementation. Few bi-lateral treaties exist and despite sustained efforts, agreements on norms (and taboos) and CBMs by international and regional organizations such as the United Nations' Groups of Governmental Experts (UN GGEs), the Organization for Security and Co-operation in Europe (OSCE), and the ASEAN Regional Forum remain elusive.

Confidence-Building Measures

The content of CBMs that these organizations propose or have already implemented overlaps significantly, however, the vocabulary used in their agreements and reports varies widely and can be a hindrance to successful communication between stakeholders (Radunovic 2017: 5/6). The UN GGE report of 2015 lays the foundation for binding norms and CBMs for the international community, and encompasses, inter alia, the following points: To respect state

sovereignty and international law, including the agreement to abide by the principle of non-intervention, to protect and refrain from targeting critical infrastructure, to enhance information-sharing and cooperation of incident response teams, and capacity building (United Nations General Assembly 2015). The OSCE has also formulated a framework for its participating States, focusing more on the necessity to find a common language and communication channels, bodies and committees for co-operation to facilitate the exchange of information and to share best practices (Ministerial Council of the Organization for Security and Co-operation in Europe 2016, 2017, Permanent Council of the Organization for Security and Co-operation in Europe 2012, 2013, 2016). The Atlantic Council identifies four broad categories for CBMs: Collaboration, crisis management, restraint, and engagement measures (Healey et al. 2014). It proposes "joint international investigations into major cyber incidents" (ibid.: 4), communication channels between nation states including the alignment of cyber emergency response teams (CERTs), hotlines and norms (ibid.).

Bi-Lateral Agreements

While numerous international and regional projects and discussions on CBMs are under way, bi-lateral agreements have not been as prevalent in the debate. The United States Department of State has summarized a few key aspects of Russia's, China's, Brazil's and India's cyber strategies and where they differ in their views on international cyber norms and taboos (Department of State International 2016). This helps the United States (US) to identify the areas in which to deter actions and behaviors of these states and to identify areas in which diplomacy and co-operation should be the preferred option. The US has bi-lateral cyber agreements with China, Russia and India, while China and Russia as well as India and Russia also signed agreements. Whether bi-lateral treaties foster or rather hinder further international co-operation is

contested. They could "feed into and fuel each other" (Radunovic 2017: 12) or "create suspicion and diminish confidence of those not directly involved" (Pawlak 2016: 149).

There is a need in the international community for a cyber rulebook, with private companies such as Microsoft even calling for a "Digital Geneva Convention" (Smith 2017). In 2013, twenty international law scholars and practitioners published the Tallinn Manual, an important milestone for the development of binding norms and rules as part of international law (Schmitt 2013). So far, however, the Tallinn Manual is merely a scientific effort, as nation states struggle to find common ground even on the bi-lateral level.

DETERRENCE IN CYBERSPACE

There is a wide range of literature on deterrence theory in cyberspace. This section will briefly introduce its two main categories, deterrence by retaliation and deterrence by denial, and will discuss the addition of two more cyber-specific dimensions, entanglement, and norms and taboos. Deterrence is generally defined as "dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit" (Nye Jr. 2017).

Deterrence by retaliation revolves around the basic notion of punishing an attacker by threatening or executing a counterstrike that will make an attack less feasible and more costly for the attacker, hence reducing the incentives for aggression (Goodman 2010).

Cyber deterrence by denial can be interpreted in two different ways: Building defense structures, resilience and capacity to recover, as well as denying adversaries access to resources, knowledge and hardware. Denial by defense works in a way that anticipates attacks, knowing the capabilities and preferred attack methods of adversaries, and finds ways to make systems more secure. This means, generally speaking, the detection of vulnerabilities and lowering risk. By making a state's systems and infrastructure less penetrable and more secure, the adversary's cost-

benefit ratio is altered, increasing their effort, resources and time involved to attack and reducing the rewards of such an attack. Denial by restricted access is less feasible in today's globalised world, however, according to Kenneth Geers (2010), it can be successful, given that three basic requirements are fulfilled: capability, communication and credibility: "Deterrence by denial is a strategy in which an adversary is physically prevented from acquiring a threatening technology" (Geers 2010). Geers admits that this interpretation of deterrence by denial has better chances of success in the prevention of nuclear war rather than a cyber war since denying access to nuclear technologies and materials is much easier than restricting access to cyber technologies and tools.

Entanglement, Norms and Taboos

There are two more factors of deterrence that can be viewed as independent influencers: Entanglement, and norms and taboos. Some scholars believe these to be "simply different instances of deterrence by retaliation" (Taddeo 2017) and that "[t]he commonality between all [..] is the reinforcement of deterrence by punishment. Each occurs in a slightly different way, but all seek to punish and curb behavior by adding a social cost" (Ryan 2017). Deterrence by entanglement is, indeed, an indicator of deterrence by retaliation, more specifically, of the success or failure of deterrence by retaliation. The more entangled two actors are on the economic and political level, the more likely it is that they can be deterred by retaliation.

When looking at deterrence by norms and taboos, however, the comparison to deterrence by retaliation is not as accurate. Norms and taboos are essentially diplomatic tools and a matter of bi-lateral and multi-lateral agreements. The taboo of attacking a state's critical infrastructure, for instance, is the result of international co-operation. This norm, however, seems to only apply to adversaries with relatively equal standing and capabilities, not nation states that are in a superior position or within their sphere of influence, as in the case of the Russian attack on the Ukrainian

electric power grid (Connell and Vogler 2017; Lee, Assante and Conway 2016). The assumption is that more deterrence is needed so as to ensure that the threshold of credible retaliation cannot be crossed. Deterring by norms and taboos, however, requires not only fear of punishment and consequences should they be ignored, but also a common environment for these norms and taboos to exist in, and measures of trust and confidence. Norms and taboos are, thus, a component of deterrence as well as international cooperation and diplomacy.

DETERRENCE AND DIPLOMACY: A COMBINED APPROACH

Deterrence theory has always been a matter of debate between historians, political and social scientists, especially with regard to its stand-alone effects. Some may argue that deterrence alone can be effective, especially when the nation state exerting power is superior in terms of their capabilities. The failure of deterrence, then, in turn, is seen as a consequence of its low intensity or non-credible implementation and execution. This is a dangerous and erroneous assumption. Robert Kagan (2016; 2017), in this context, claims that sophisticated, high-end deterrence works as long as the adversary is afraid to operate on a high level in an openly aggressive manner, and as long as high-end deterrence is credible and there is no doubt about possible retaliatory actions.

Applying Traditional Approaches to Cyber Space

In the context of cyber, the dimensions of both deterrence and diplomacy are widened and have to be understood before analyzing their intertwined nature. Traditional approaches limit retaliatory, defensive and diplomatic responses to the non-digital world. Options may include economic sanctions, political disengagement by closing embassies and ending diplomatic relations, and even kinetic responses, military engagement and anti-missile systems. The nature of cyber space, however, enables complex hybrid response options. Hence, the added dimension of cyber space allows deterrence and diplomacy to be carried out in a cross-domain field:

Traditional military threats, for example, can be responded to in the cyber domain. Cyber threats can be responded to in the cyber domain or the traditional military, economic and diplomatic domain. It is important to understand that cyber deterrence and cyber diplomacy are not solely restricted to the digital sphere.

The attempt to transfer the traditional comprehensive approach to the cyber sphere has to happen in a comprehensive manner as well, considering both deterrence and diplomacy in their interdependence. Conjunction of both concepts is necessary, however, the importance and relevance of the specific variables involved differs. It is inevitable to weigh the importance of these variables according to the context and the nature of the threat. In order to make the arguments more tangible, we examined two cases, i.e. the US-China cyber treaty and alleged Russian influence in the 2016 US presidential election.

US – China Cyber Espionage Agreement

In the run-up to the 2015 US–China Cyber Espionage Agreement, the Obama administration had repeatedly stressed that the US was not engaging in economic cyber espionage for commercial benefits and that the theft of intellectual property by China had to come to an end (Brown and Yung 2017a; Obama 2015). For the examination of the general thesis of this paper, it is crucial to look at the unsuccessful approaches that were introduced in the years leading up to the treaty, and the reasons for the relative success that manifested itself in the bi-lateral cyber agreement.

As deterrent measures, the US indicted five members of the People's Liberation Army in 2014, an action which was ultimately unsuccessful at deterring the threat (Sanger 2015). Again, in 2015, the US made a credible threat of imposing economic sanctions, an action which played a major role in bringing China to the negotiation table (Nakashima 2015). The fear of reputational and economic damage in combination with years of cooperative engagement (Department of

State International 2016) resulted in a bi-lateral agreement to lower risk of future theft and to mitigate that reputational damage: "Another reason for China's willingness to enter into the agreement […] is the growing reluctance of U.S. companies to locate in China, particularly in the case of research and development centers. An increasingly unfavorable reputation regarding the theft of intellectual property from companies located in China may have been dampening enthusiasm for continued investment in China. In the long run, this could be a blow to China's continued economic development" (Brown and Yung 2017b).

There are three factors that are unique to the US - China scenario: A low likelihood of kinetic military action, high economic entanglement, and potential reputational damage. All three variables include soft and hard power components, which form a complex picture of US - China cyber relations. If the threat of commercial cyber espionage, in this specific case, was solely deterred or solely appeased, the cost for both actors would have inevitably gone up. Appeasement would have led to a continuous or elevated frequency of cyber attacks by China, thus raising the cost for American companies and citizens. Deterrence would have led to economic sanctions against China, thus threatening the interdependent economic prosperity of both and raising the reputational cost for economic investment in China (Brown & Yung 2017b).

Scientific scholars argue that the relatively positive outcome of this case is owed to successful deterrence by retaliation, denial and, most importantly, entanglement: "Unlike the single strand of military interdependence that linked the U.S. and the Soviet Union in the Cold War, the United States, China, and other countries are entangled in multiple networks. China, for example, would itself lose from an attack that severely damaged the American economy, and visa versa" (Nye Jr. 2010: 16f.). Since China is the United States' largest trading partner (United States Census Bureau 2018), using economic deterrence measures was successful in leading both

parties to a diplomatic agreement. Conversely, the Russian Federation has proven to be less vulnerable to such deterrence measures because of its relatively low engagement in international trade with the U.S. (ibid.). Thus, the composition of deterrent and diplomatic measures has to be adjusted on a case-to-case basis.

Surely, the extension of deterrence theory to include economic and political entanglement is important, and can, in part, explain why China agreed to a cyber security treaty. It is evident, however, that the diplomatic factor can also not be ignored in the analysis of this case: In traditional threat scenarios, the outcome of a deterrence or diplomatic effort would be physically visible and violations immediately observable through the removal of missiles or heavy machinery, disarmament agreements, the retreat of soldiers and so forth. In cyberspace, an agreement such as the one between China and the US requires trust and confidence that the adversary will abide by the rules and comply with the treaty. Consequently, even with low levels of trust between the two nation states in this case, a bi-lateral agreement was, nevertheless, seen as the best alternative to economic sanctions. Years after the agreement was signed, there are now indications that the diplomatic efforts combined with deterrence by retaliation and entanglement, have indeed significantly reduced economic cyber espionage for commercial gain, and that future agreements could build on and improve upon the US – China Cyber Espionage Agreement (Harold 2016; Louie 2017).

External Influences in the 2016 US Presidential Election

During the 2016 US presidential elections, the Russian Federation launched a well-planned massive social media campaign to sow discord by spreading distrust for candidates and the political system in the United States. According to the Mueller indictment (United States of America v. Viktor Borisovich Netyksho et al. 2018), the planning cost millions of dollars and

involved scores of Russian operatives who were on US soil. The campaign involved use of social media sites such as Facebook, Twitter, Instagram, and YouTube, where bot accounts were set up for disseminating misleading, politically sensitive information, for instance, promoting Donald Trump and disparaging Hillary Clinton. The operatives infiltrated the Democratic National Committee (DNC) and the Democratic Congressional Campaign Committee's networks by injecting malware which allowed them to install keyloggers and steal passwords of campaign aides and servers. Once in the network, hackers were able to steal confidential documents and emails from the DNC servers. They released the stolen information strategically to discredit Hillary Clinton and derail her campaign.

In the case of Russia interfering with the 2016 US election, both deterrence and diplomacy failed, despite warnings by the Obama administration that further action by the Russian government would have consequences, and despite efforts to covertly increase the cost for Russia to launch attacks (Landler and Sanger 2016; Ewing 2018). With regard to deterrence, retaliatory threats were largely ineffective due to a lack of credibility and entanglement between the US and Russia. Additionally, the US lacked defensive capabilities, lowering the effectiveness of deterrence by denial. At the same time, diplomatic responses, such as expelling diplomatic personnel, and face to face conversations and warnings between US president Barack Obama and Russian president Vladimir Putin were likely perceived as non-credible, low risk threats by the Russian Federation (Carson 2017). To protect itself in the future, the US will need to invest in its defensive capabilities, thus improving deterrence by denial measures. This will include improving the security of government and campaign networks and servers, as well as raising awareness amongst diplomats and politicians like Hillary Clinton on how to best protect their data. A combination of securing networks and building defensive structures for political

institutions, and entering a diplomatic dialogue with the Russian Federation on norms and taboos on the use of cyber technologies will be the first step towards normalizing their cyber relations.

While the tools for launching this Russian operation are not novel, the planning, scale, and coordination of the operation was astoundingly meticulous, making it so successful. While election meddling and its impact on this campaign in the 2016 US elections is not in dispute anymore, attribution of the individual hackers and their sponsors is not completely clear. Therein lies the problem; with uncertainty in identifying sponsors and perpetrators of such activities, it is difficult to deter them in the future as discussed in the following section.

DISCUSSION

We argue that deterrence and diplomacy have to go hand in hand in order to prevent a cyber war or escalation of the use of cyber weapons. The adoption of traditional theories to the cyber realm is under way; however, this process is accompanied by doubt and concern about its feasibility and effectiveness. Cyber weapons are inexpensive and can be disseminated fast, the attribution of attacks is hard, and secrecy around available tools, intelligence and knowledge blur the potential defensive and offensive possibilities.

Attribution is a problem for both cyber deterrence and diplomacy. In order to identify a measured diplomatic, economic, military or cyber response to an incident without becoming the aggressor or creating new adversaries, attribution is key (Bendiek and Metzger 2015). Appropriate retaliation as well as diplomatic consequences to cyber attacks have long been considered problematic due to the ambiguities of their origins. It has been argued that attribution in cyberspace is, in fact, not impossible anymore (ibid.). Yet the risk of escalation and a cyber arms race remains. In the realm of diplomacy and CBMs, the creation of a multi-lateral cyber adjudication and attribution council has been proposed (Healey et al. 2014), although

cooperation on this level seems quite unlikely in the current international atmosphere. When looking at the attribution problem as a shared obstacle to both effective deterrence and effective diplomacy, the combined approach might help to find creative solutions. Norms and regulations could, for instance, provide a framework for binding agreements, which, in turn, will make retaliatory and defensive deterrence more feasible, as the accepted norms can be used to facilitate attribution and cooperation to identify culprits and enhance the credibility of deterrence.

Attribution is not the only challenge with regard to cyber deterrence and CBMs. Nation states – both the ones carrying out attacks and the ones affected by them – operate under a level of confidentiality which was not as prevalent in the Cold War. Nuclear deterrence by retaliation as well as by denial was largely based on the credibility of the claim that a state actor had the capabilities and the know-how to retaliate or defend itself against an attack. Similarly, CBMs, in the traditional sense, would include clear and strict rules, norms and practices, meaning that a state actor could be called out on a particular action or a certain behavior that was not in compliance with these agreed-upon rules and norms. It is not easy to hide incidents or defensive military systems in a non-digital, physical environment. In cyberspace, however, secrecy appears to be an inherent method of deterrence and cooperation, both in a negative and positive sense. "No national strategy exists for deterring cyberattacks by retaliation [..], with little indication available as to what sorts of retaliation are planned or under development" (Morgan 2010, 57). In addition to complicating deterrence by retaliation, deterrence by denial in cyberspace shifts from highly visible movements of heavy machinery and the deployment of anti-missile systems to the secret development of cyber weapons. If the defender knows the capabilities of the adversary, vectors of attack can be closed at relatively low cost and high speed compared to the kinetic and economic sphere, creating a strong incentive to keep cyber capabilities and know-how secret.

This is a challenge, as cyber deterrence relies increasingly on psychological manipulation and signaling of capabilities that are not visible, making it more difficult to convey credible retaliatory and defensive capabilities. Diplomatic advances, in turn, become harder to achieve, as secrecy, anonymity and difficulty of attribution complicate confidence-building and trust.

To facilitate the comprehensive approach suggested in this paper, it is important to note that cyber conflicts cannot be equated with military or economic confrontations, especially regarding methods of conflict prevention and resolution. Depending on the variables outlined above, including economic and political entanglement, defensive capabilities and power relations between the conflict parties, an appropriate balance of deterrent and diplomatic efforts to mitigate risk of escalation can be found.

One of the most challenging balancing acts will be to achieve sophisticated, high-end deterrence without escalating the conflict and actively accelerating the cyber arms race. Nation states will need to make credible claims about their capabilities in the digital sphere to deter adversaries, while building trust and confidence to ensure that their adversaries know they will not launch a preemptive attack and will not strike without an independent international authority assessing and attributing the attack.

CONCLUSIONS

In the political discourse on cyber weapons and its implications for new types of warfare in the international arena, there are various approaches, ranging from cyber deterrence strategies to bilateral and multilateral treaties to prevent attacks. While international and regional organizations focus their efforts on drafting confidence-building measures, norms and cooperative strategies, military organizations and domestic defense agencies largely emphasize deterrence measures and dissuasive tactics. During the Cold War, both deterrence and diplomacy

played an enormous role in preventing military and nuclear confrontation. Therefore, deterrence and diplomacy should also not be seen as two independently existing methods to prevent a cyber war, but should go hand in hand in an effort to prevent cyber conflicts.

If traditional approaches to deterring, mitigating and diplomatically preventing threats are transferred to cyberspace, they need to be adapted to the entirety of complexities of the modern cyber era. Historically, a combination of deterrence and diplomacy has been used to deescalate conflict in the international arena. Therefore, adopting single aspects of these concepts to cyber warfare is not recommendable. Deterrence theory has already been augmented to meet some of the new challenges of cyber and information technologies, however, in order to account for the realities of conflict in cyberspace, and in order to make well-grounded and informed policy recommendations to governments, the intertwined nature of deterrence and international diplomacy as well as the intricacies of cross-domain hybrid warfare have to be accounted for.

It is impossible to keep all the variables in mind at all times, and our analysis limits the scope to nation state actors and certain aspects of deterrence theory and international diplomacy. There is no grand strategy, no perfect, universal, one-size-fits-all solution, but there can be a vision that encompasses a fair amount of sensible strategic actions that can lead to successful deterrence and co-operation between nation states in cyberspace. Whether State A leans more towards deterrence or diplomacy largely depends on the context and history of the relationship with State B. Thus, the variables in both concepts need to be examined on a case-to-case basis. Sometimes, deterrence strategies will be predominant, other times diplomacy will be more useful or effective. The balance and weight of each variable can shift over time, as the relationship between states evolves, improves or deteriorates. It is a fluid and flexible concept. The crucial point, however, is that both approaches have to come into play in order to prevent conflict.

REFERENCES

[1] Bendiek, A., and Metzger, T. 2015. Deterrence Theory in the Cyber-Century, Berlin: Stiftung Wissenschaft und Politik.

[2] Brown, G., and Yung, C. D. 2017a. "Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace," The Diplomat. (https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/, accessed February 20, 2018).

[3] Brown, G., and Yung, C. D. 2017b. "Evaluating the US-China Cybersecurity Agreement, Part 3," The Diplomat. (https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-3/, accessed February 20, 2018).

[4] Carson, A. 2017. "Obama Used Covert Retaliation in Response to Russian Election Meddling. Here's Why.," The Washington Post. (https://www.washingtonpost.com/news/monkey-cage/wp/2017/06/29/obama-used-covert-retaliation-in-response-to-russian-election-meddling-heres-why/?noredirect=on&utm_term=.020d9d5bb97d, accessed July 20, 2018).

[5] Connell, M., and Vogler, S. 2017. "Russia's Approach to Cyber Warfare," CNA Analysis and Solutions. (http://www.dtic.mil/dtic/tr/fulltext/u2/1032208.pdf, accessed July 20, 2018).

[6] Department of State International. 2016. "Cyberspace Policy Strategy," No. Public Law 114-112, Division N, Title IV, Section 402.

[7] Ewing, P. 2018. "FACT CHECK: Why Didn't Obama Stop Russia's Election Interference In 2016?," National Public Radio. (https://www.npr.org/2018/02/21/587614043/fact-check-why-didnt-obama-stop-russia-s-election-interference-in-2016, accessed July 20, 2018).

[8] Geers, K. 2010. The Challenge of Cyber Attack Deterrence, Tallinn, Estonia: Elsevier, Naval Criminal Investigative Service, Cooperative Cyber Defence Centre of Excellence.

[9] Goodman, W. 2010. "Cyber Deterrence: Tougher in Theory than in Practice?," Defense Technical Information Center, Senate (United States) Washington D.C. Committee on Armed Services.

[10] Harold, S. W. 2016. "The U.S.-China Cyber Agreement: A Good First Step." (https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html, accessed February 20, 2018).

[11] Healey, J., Mallery, J. C., Jordan, K. T., and Youd, N. V. 2014. "Confidence-Building Measures in Cyberspace," Atlantic Council, Brent Scowcroft Center on International Security, National Defence Council.

[12] Kagan, R. 2016. Deterrence in the 21st Century, presented at the Panel Discussion: Center for Strategic and International Studies. (https://www.csis.org/events/deterrence-21st-century).

[13] Kagan, R. 2017. "Backing Into World War III," Foreign Policy. (https://foreignpolicy.com/2017/02/06/backing-into-world-war-iii-russia-china-trump-obama/, accessed February 20, 2018).

[14] Landler, M., and Sanger, D. E. 2016. "Obama Says He Told Putin: 'Cut It Out' on Hacking," The New York Times. (https://www.nytimes.com/2016/12/16/us/politics/obama-putin-hacking-news-conference.html, accessed July 20, 2018).

[15] Lee, R. M., Assante, M. J., and Conway, T. 2016. "TLP: White. Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case," E-ISAC.

[16] Louie, C. 2017. "U.S.-China Cybersecurity Cooperation," The Henry M. Jackson School of International Studies. (https://jsis.washington.edu/news/u-s-china-cybersecurity-cooperation/, accessed February 20, 2018).

[17] Ministerial Council of the Organization for Security and Co-operation in Europe. 2016. "Decision No. 5/16: OSCE Efforts Related to Reducing the Risks of Conflict Stemming from the Use of Information and Communication Technologies."

[18] Ministerial Council of the Organization for Security and Co-operation in Europe. 2017. "Decision No. 5/17: Enhancing OSCE Efforts to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies."

[19] Morgan, P. M. 2010. Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm, University of California, Irvine: Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy; Committee on Deterring Cyberattacks; National Research Council.

[20] Nakashima, E. 2015. "U.S. Developing Sanctions against China over Cyberthefts," Washington Post. (https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html).

[21] Nye Jr., J. S. 2010. "Cyber Power," Harvard Kennedy School: Belfer Center for Science and International Affairs. (http://www.dtic.mil/dtic/tr/fulltext/u2/a522626.pdf).

[22] Nye Jr., J. S. 2017. "Deterrence and Dissuasion in Cyberspace," International Security (41:3).

[23] Obama, B. 2015. "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference," Whitehouse.Gov. (https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint, accessed February 20, 2018).

[24] Pawlak, P. 2016. "Confidence-Building Measures in Cyberspace: Current Debates and Trends," International Cyber Norms: Legal, Policy & Industry Perspectives.

[25] Permanent Council of the Organization for Security and Co-operation in Europe. 2012. "Decision No. 1039: Development of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies," No. 1039.

[26] Permanent Council of the Organization for Security and Co-operation in Europe. 2013. "Decision No. 1106: Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies."

[27] Permanent Council of the Organization for Security and Co-operation in Europe. 2016. "Decision No. 1202: OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies."

[28] Radunovic, V. 2017. "Towards a Secure Cyberspace via Regional Co-Operation," DiploFoundation.

[29] Ryan, N. J. 2017. "Five Kinds of Cyber Deterrence," Philosophy & Technology. (https://doi.org/10.1007/s13347-016-0251-1).

[30] Sanger, D. E. 2015. "U.S. Decides to Retaliate Against China's Hacking," The New York Times. (https://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html).

[31] Schmitt, M. N. (ed.). 2013. "Tallinn Manual on the International Law Applicable to Cyber Warfare," Cambridge University Press.

[32] Smith, B. 2017. "The Need for a Digital Geneva Convention," Microsoft on the Issues. (https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/, accessed February 20, 2018).

[33] Taddeo, M. 2017. "The Limits of Deterrence Theory in Cyberspace," Philosophy & Technology. (https://doi.org/10.1007/s13347-017-0290-2).

[34] United Nations General Assembly. 2015. "Group of Governmental Expert on Developments in the Field of Information and Telecommunications in the Context of International Security," No. A/70/174. (http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174).

[35] United States Census Bureau. 2018. "Foreign Trade." (https://www.census.gov/foreign-trade/statistics/highlights/toppartners.html, accessed July 20, 2018).

[36] United States of America v. Viktor Borisovich Netyksho et al. 2018. United States District Court for the District of Columbia. (https://www.justice.gov/file/1080281/download, accessed July 20, 2018).