Masyarakat, Kebudayaan dan Politik
https://doi.org/10.20473/mkp.V33I42020.331-338

Approaches to international information security and the discourse of cyberspace

Pendekatan keamanan informasi internasional dan wacana dunia maya

Tauqeer Hussain Sargana[1]*, Mujahid Hussain Sargana[2], & Muhammad Anns[3]
[1]Department of Politics and International Relations, Faculty of Social Sciences, International Islamic University Islamabad
[2]Department of Humanities and Social Sciences, Bahria University
[3]Department of Criminology, Institute of Social and Cultural Studies, University of the Punjab
Address: [1]Sector H-10, New Campus Islamabad, Pakistan
[2]Shangrilla Road, Sector E-8, Islamabad, Pakistan
[3]Canal Road, Quaid-i-Azam Campus, Lahore, Punjab, Pakistan
E-mail: tauqeer.hussain@iiu.edu.pk*, mujahid_hussain70@yahoo.com, & kharalmureed@gmail.com

Article History: Received 7 July 2020; Accepted 10 October 2020; Published Online 26 October 2020

Abstract

This paper investigates the notion of sovereignty and territorial integrity of states in cyberspace by carefully examining the information security debate. Nowadays, issues related to infosec are posing fundamental challenges to the sovereignty and territorial integrity of nation-states. Our analysis has attempted to answer the critical question, which aspect makes infosec the most pressing issue of the 21st century? The United States, The Russian Federation, and China are the three technologically superior nations and are included in the study to compare their understanding of infosec issues. The authors have typically relied on their expertise to interpret primary and secondary data because of descriptive discourse. Moreover, the study is efficiently conducted through a deductive approach and has applied non-kineticism as a theoretical model. The results showed that due to the compelling non-kinetic application of infosec, the debate at international forums had become a victim of geopolitical considerations. Results also revealed that the discourse of infosec needs to be disassociated from social freedom as it has been adopted for military application and requires a national security perspective to confine the course of security implications. In abstract, the notion of infosec has given birth to new contestation in the domain of cyberspace that altogether would lead the competition into the 'digital battlefield.'

Keywords: solarium commission; cyberspace; non-kineticism; information security; cyber sovereignty

Abstrak

Artikel ini menelusuri konsep kedaulatan dan integritas teritorial negara dalam ruang siber dengan analisa mengenai keamanan informasi. Saat ini, isu yang berkenaan dengan keamanan informasi menjadi salah satu tantangan utama dalam pemaknaan kedaulatan dan integritas territorial negara bangsa. Analisis bertujuan untuk menjawab pertanyaan mendasar mengenai aspek apa saja yang membuat keamanan informasi menjadi isu paling penting di abad 21? Subjek riset adalah Amerika Serikat, Federasi Rusia, dan Cina, sebagai tiga negara yang memiliki kemampuan teknologi yang mumpuni guna mendapatkan perbandingan pemahaman masing-masing negara atas isu keamanan informasi. Data primer dan sekunder diinterpretasikan melalui metode wacana deskfriptif. Studi ini dilaksanakan melalui pendekatan deduktif dengan model teori non-kinetis. Hasil penelitian menunjukkan bahwa metode non-kinetis dalam menelusuri isu keamanan informasi, perdebatan dalam forum internasional banyak terdampak oleh pertimbangan geopolitik. Studi ini juga menemukan bahwa diskursus mengenai keamanan informasi perlu dipisahkan dari konsep kebebasan sosial. Secara garis besar, isu keamanan informasi telah melahirkan kontestasi ruang siber yang dapat menciptakan 'medan perang digital'.

Kata kunci: *komisi solarium; dunia maya; non-kinetikisme; informasi keamanan; kedaulatan dunia maya*

Introduction

The issue of systematic cyber risks in the age of information revolution has brought further dimensions to state safety (Cavelty 2013). The high spectrum of threats associated with international infosec demands a robust alternative approach to deal with the evolving cyber risks. It has been a well-taken security threat, particularly by the developed nations. The front runners of infosec are

The United States, The Russian Federation, and the People's Republic of China. In the absence of an international framework to address the legality of information protocols, The United States gained the lead in 2019 and established the Cyberspace Solarium Commission (Rosenberger 2020).

On March 11, 2020, the commission issued its report that inked the so-called strategy necessary to defend The United States' interest against cyberattacks. The statement also charted out 75 recommendations and called them "layered cyber deterrence" with goals to minimize the probability and impact of cyberattacks of significant consequences (Klimburg 2020). Alongside strategies and recommendations, the article also proposed the necessary legislation to implement the policy. The Solarium Commission set up under the 2019 National Defense Authorization Act, which obtained its reference from President Eisenhower 1953 "Project Solarium." It establishes to address a nuclear threat as the topmost challenge to The United States National Security (Townsend 2020). The strategic reflection of national security that Eisenhower dealt with project solarium shifted to an increased insecurity level. As a result, the state enterprise as a whole got changed into a battlefield. Keeping in view this modern battlefield and the course of information technology, many in The United States were skeptical about their preparedness to deal with cyber conflict (Sanger 2018). Feaver & Inboden (2018), suggesting the turnover in The United States National Security approach and proposed highlighting the threats of cyberspace and referred to the Solarium Project of 1953, and it contested the policy alteration as the strategic paradigm shift. It only took a year to witness the proposed strategic paradigm shift, when in 2019, the Cyberspace Solarium Commission establishes. Subsequently, on March 11, 2020, the commission submitted its report. The dilemma of cyber threats is the primary national security risk for The United States (Goel 2020).

The question is why cyber threat took over the traditional notion of security that The United States had been in contestation with, and who are the bidders of the digital battlefield? First of all, it is essential to underscore the context of cyber fears. It is not only a domain however equally an instrument that, unlike strategic weapons, which require enormous resources—the cyber tools are cheap and available to anyone with low economic resources (Bieda & Halawi 2015). Therefore, these cyber tools are a ready-made carnage recipe that the non-state actors can wreak from an uncertain origin. The availability of the same tools to modern and technologically advanced nations can cause greater instability to the global economy and international peace and security (Leuprecht et al. 2019).

Unlike the strategic weaponry whose course is traceable and only included in the military inventory of the most powerful nations, the hands behind the execution of cyber-attacks are challenging to trace and identify (Pytlak & Mitchell 2016). Hence, neither deterrence nor an immediate cyber trajectory trial qualifies traditional military strategies to establish clear communication. Cyber-attacks are happening daily by nation-states on the non-state actors, and by the non-state actors on nation-states. In the cyberspace, even the known thresholds are very much compromised (Hayward 2017). Since machines can be controlled, however, human minds cannot be controlled, who knows the attack was executed by one of its national institutions to sabotage national security? The absence of an international mechanism to tackle the sensitivity of evolving cyberspace with associated challenges is a critical aspect. This research article is striving to highlight these concerns. It is not only The United States that is facing the spectrum of insecurity in cyberspace. Instead, China and Russia have shared their concerns about international infosec (Singer & Friedman 2014). The disagreement between these three being the top bidders of cyberspace creates complexity and confusion to address the problem through a legitimate order (Nolan 2015). Their contestation on the legality of the subject makes the matter worse. Each side presents its version of international infosec that all together creates parallel poles of ideas.

This article has attempted to objectively present these top bidders of cyberspace's perspectives with the approaches floated at international forums. The following part of the study describes the methods and materials adopted to base the research's methodological underpinnings. The section after that explains the results and analysis. The latter portion concludes the theoretical dilemma and the practical issues associated with the discourse of international infosec.

Research Method

The study is based on the deductive premise, which contextualizes the Cyberspace Solarium Commission's preamble that The United States established in 2019. It makes the analysis descriptive in nature and allows the case study approach to analyze three influential nations facing cyberspace's dilemma. Different connotations of cyberspace within the international infosec domain put forward The United States, China, and Russia as the digital battlefield's frontrunners. The hypothetical assumption of the research infers that infosec has given rise to a digital battlefield, far more potent than the traditional combat zone. It places cyberspace between discourse and dilemma, which is why infosec issues are posing fundamental challenges to the sovereignty and territorial integrity of nation-states.

The study's interpretive part is subjective and relied on secondary data, including published information in research journals and online news reporting. The United States Cyberspace Solarium Commission report is considered the core document to carry out the analysis part to sustain the study's primary outlook; the summary was released on March 11, 2020. The authors have deliberated explanatory pretext to shed light on the technologically superior nations. These nations' strong political, diplomatic, economic, and military power can exploit the digital space. The non-kinetic application of infosec contextualized the data collection process. Due to the compelling non-kinetic application of infosec, the debate at international forums has become a victim of geopolitical considerations. Today, the infosec discourse needs to be disassociated from global norms, as the predominant feature of its practice has begun to shape the military environment.

Results and Discussion

In October 2019, Clement (2019), in Statista, reported that more than 4.48 billion people worldwide were on the internet. It almost makes half of the population, an active consumer of the internet that, in turn, qualifies the topic of infosec as a top-priority issue in the age of computing. Before the Statista Report, back in 2017, the Norton Cybercrime had also published the data where they claimed that about 978 million people in 20 countries were affected by cybercrime (Norton Cyber Security 2017). Nowadays, the rise in cyber-crimes has affected every government in the world. People from all corners of life face different types of cybercrimes that find their ways through social media sites, mobile devices, and computing devices. Only in 2017, around US$172 billion lost due to cybercrimes that, on average, cost US$142 to an individual victim (Norton Cyber Security 2017). Interestingly, this aspect of cybercrime is less expensive than crime in cyberspace, which is purely a non-kinetic warfare domain. Many countries in the world are still unaware of the future and, without sufficient understanding, are unconscious regarding cyberspace threats. The 2020 Solarium Commission Report suggests that The United States and few European Nations have begun the policy process to mechanize infosec; however, the rest still lacks behind. In countries without any awareness or security guidelines, cyberspace's vulnerability would clutch their nations' very sovereignty and future. According to France Diplomatie (2019):

> "New destructive practices are developing in cyberspace, including criminal use of the internet (cybercrime), for terrorist purposes; large-scale propagation of false information; espionage for political or economic ends; and attacks on critical infrastructure (transport, energy, communication) for sabotage."

The emerging dynamics of cybersecurity have opened new avenues of war and policy dialogues to counter complex challenges associated with the threat. A few of the dimensions are analyzed below:

Cyber power and international competition

The 21st-century power matrix includes the military and the economy as elements of power rather than culture, human resources, and above all, technology has redefined the foundation of international competition. Revelations by Edward Snowden are enough to open the world's eyes, particularly in

The United States (Weinstein 2014). Cyber-attacks in Eastern European states like Ukraine, Estonia, and Georgia might be traced back to Moscow and tangibly reflect The Russian Federation's powerful cyber tools (Nakashima 2018). Parallel to that, the top four world internet companies belong to China that includes: JD, Tencent, Alibaba, and Baidu, which are defining the future of artificial intelligence with that of the Chinese internet economy (Jia et al. 2018). It makes The United States one of the most expensive competitors that have now formally considered the cyberspace as the topmost priority of The United States National Security. The participation of developed nations in the sphere of cyberspace has started up an international competition that, in turn, has evolved a new domain of digital warfare. Where massive investment in cyberspace allows a state to increase the opportunities, it also creates a security dilemma for the competitive stakeholders that reciprocate their cyber capacities. It initiates the vicious cycle between cyber sovereignty and cyber freedom.

Cyber sovereignty vs. cyber freedom

The 21st-century has manifolded the technological context opportunities for human development with industrial production to enhance warfare capabilities. Cyberspace has boosted an unpredictable spectrum of national security where ultimate peace and stability are considered rare possibilities. This understanding had made not only cyberspace the fifth domain of strategic forces; however, it also increased the international competition between great powers (Lynn III 2010). The competition within the players of cyberspace has also distinguished the understanding of the concept itself. For example, Chinese and Russian point of view could be labeled as "cyber sovereignty" (Shen 2016), contrary to the idea of "cyber freedom" that has been a permanent feature of western political thought. The apprehensions of both Chinese and Russian observers consider that the West can meddle in developing nations' internal affairs through the pretext of cyber freedom. American diplomacy with Western culture found an ideal route through social media platforms to organize controlled chaos within the target nations that, with little support, can be materialized into color revolutions. The ill-understanding of developing nations in the subjective understanding of freedom of speech also makes them vulnerable to color revolutions. The nations have postulated this pretext with controlled governments; hence The Russian Federation and China are seriously advocating the idea of cyber freedom. Alternatively, the idea of cyber sovereignty gives states the required legitimacy in governing cyberspace's norms. Interestingly, the idea has already been underscored by international forums like the United Nations Group of Governmental Experts (UNGGE) on infosec (Davis & Lewis 2019) as well as by North Atlantic Treaty Organization (NATO) (Schmitt 2013) and The United States (Koh 2012). The plan seems practical; however, the concept's meaning is still disputed between the bidders and competitors. It is essential to highlight that both schemes must introduce necessary reforms to signify internet development regulation and establish cyberspace norms.

Multilateral approach vs. multi-stakeholder approach

The multilateral approach vs. multi-stakeholder phenomenon is indifferent from the above discourse of cyber sovereignty vs. cyber freedom. The only difference is that both approaches give a new outlook to the ongoing competition in defining cyberspace's regulatory context. For example, in the multi-stakeholder approach, which is the idea of western nations, particularly of The United States, the actors' such tech companies, individuals, and the internet giants would have played a key role in regulating the global cyberspace. It dilutes the role of the governments and makes cyberspace another market for multinational corporations. Contrary to this approach, China and Russia find the multilateral approach more feasible to regulate cyberspace, which provides governments the authority to develop checks and balances to control the cyber traffic in line with each stakeholder (Rosenbach & Chong 2019). The debate is ongoing, and the security dilemma is paving undue uncertainty into the spectrum of cyberspace. The Chinese authorities have even rightly picked up that in 2017, China calls for enhanced communication and cooperation among all stakeholders, including governments, international organizations, Internet companies, technological communities, non-governmental institutions, and citizens. Relevant efforts should reflect broad participation, sound management, and democratic decision-making. All stakeholders should contribute their share

based on their capacity with governments taking the lead in internet governance, particularly public policies and security (Shaohui 2017). The world at large cannot afford further disintegration and division in global governance. Therefore, it is essential to collaborate on the point of consensus to address the growing challenges of international infosec as both approaches constitute an integral part of regularizing cyberspace with that of the internet governance model.

Cyberspace militarization

In theory, the possibility of cyberwar still contested; however, the revolution in Information and Communication Technology (ICT) has made enormous progress with application in the war theatre. The last few years are evident to underscore cyberspace militarization that has altogether given impetus to associated ideas, advancement in theoretical premises, the establishment of cyber commands, and the development of cyber tools to be used as weapons. This overall reflects a new paradigm in politics among nations. Almost three decades ago, the RAND Corporation 1996 had already identified the strategic information warfare as the pretext of 21st-century conflict (Molander et al. 1996). Subsequently, in 1997 the pace of technological advancements in communication tools predicted that the cyberwar is coming (Arquilla & Ronfeldt 1997). Continuing with the pace of changes in the dynamics of the battlefield with that of technical maneuvers, about a decade later, according to Lynn III (2010), The United States Deputy Secretary of Defense wrote:

> "As a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain of warfare. Although cyberspace is a human-made domain, it has become just as critical to military operations as the land, sea, air, and space."

Meanwhile, in June 2009, The United States successfully established a Cyber Command that was made subordinate to Strategic Command, which tasks to achieve dominance in the domain of cyberspace. It was further verified in 2012, according to Bumiller & Shanker (2012) when the Leon Panetta, The United States Defense Secretary, said:

> "The United States Department of Defense has drafted new rules of engagement in cyberspace, which would enable The United States military to respond more quickly to cyber threats."

In October 2016, according to U.S. Department of Defense (2016), the Cyber Command released the information that:

> "All 133 of The United States Cyber Command's Cyber Mission Force teams achieved initial operating capability as of October 12, 2016."

In August 2017, the Cyber Command was elevated to Unified Combatant Command (COCOM) as a sole operational command to deal with cyberspace issues and was made directly answerable to The United States Secretary of Defense (White House 2017). It occurred in the aftermath of the alleged Russian meddling of The United States presidential elections. Therefore, in the aftermath of cyber-sabotage in 2016 The United States presidential elections, the Cyber Command of The United States adopted preemptive measures during the 2018 midterm elections by launching the equivalent of a massive Distributed Denial of Service (DDOS) attack against the Internet Research Agency, throwing it offline (Lyndsey 2019). To deny any further space for cyber-sabotage on 2020 The United States presidential elections, the Cyber Command has adopted a persistent engagement, which means the cyberspace will be an arena with no sanctuary for adversaries, and military operations will have no operational pause. In other words, persistent engagement means that any action will be met swiftly with a counter-action (Lyndsey 2019).

The United States is not the only bidder of cyberspace dictum. The Russian Federation developed too the information security doctrine adopted by the Russian Information Security Committee in 2002 (Heickero 2010). The doctrine listed the cyberspace as sixth generation warfare and demanded cyber readiness by developing an upgraded cyber force called persistent engagement of The United States Cyber Command meant to compete and deter the Russian information forces. It makes the story of international infosec complex and challenging to cater to international norms.

NATO has also taken tangible steps to recognize and establish appropriate measures to prepare the domain of cyberspace. For example, in 2016, during Warsaw Summit, NATO reiterated that it would defend itself as it does in the air, on land, and at sea and focus on improving its member states (North Atlantic Treaty Organization 2016). States working to improve their international stature have already begun to invest in the field of cyberspace, which is why the apprehensions about the cyber arms race would require a parallel institutional mechanism to counter the proliferation of cyber weapons.

Conclusion

The next stage of proliferation will be seen in cyber-weapons, which may have already begun. The world must get ready to measure the consequences of the military application of digital combat. It mostly argued among the strategic community that Washington considers cyberspace as a tool to impact other states' policies. The United States initiatives in the infosec field aim to get unlimited access to cyberspace and pressure them. Russian and Chinese propagates the viewpoint that the United States is already proficient and possesses a broad spectrum of controlling cyberspace capabilities. It allows determining the threats and provides the opportunity to choose an appropriate method of engaging the rivals. Due to exceptional leverage in cyberspace with that of unfolding technological superiority, the United States has achieved a leading player in cyberspace, but altogether is accused of spreading false news about infosec with cybercrime and terrorism acts digital domain.

The story of Washington's superiority in the cyber domain does not end here. The debate around infosec also points out that through bilateral agreements, the United States initially makes her partners dependent on Western technologies, imposing on them the unbeneficial partnership in some sensitive national security areas, including military-technical cooperation. Any partner nation cannot rule out that US-sold military equipment and systems will contain hidden software that transmits data to producers and enables them to control such equipment and apparatus. A good example is the STUXNET virus used by the Americans in Iran, a joint US-Israeli operation that destroyed the centrifuges in Iran's Natanz nuclear reactor. It resulted in the hacking of the control network and then speeding up and slowing down the rate at which they spun. Before the STUXNET attack, in March 2007, a test nicknamed The United States Department of Energy conducted AURORA in an attempt to disrupt the civil electricity supply network. The experiment proved that a cyberattack—the simple insertion of malware—can not only manipulate a computer but destroy an object that the computer controls. By 2020 all these experiments have reached the highest military application and are ready to unleash their fullest destruction. It is why the International Infosec has become the most pressing issue of the 21st-century, and global nations must focus on the terrible fallout of the weaponization of cyberspace.

Acknowledgement

The researchers are thankful to International Islamic University Islamabad and Bahria University Islamabad that provided academic support to complete this research. Data were accessed from the Central Libraries of both institutions that mitigated the financial burdens, which otherwise may have created difficulty in investigating the subject matter descriptively. Through his discussions on the changing nature of warfare, Muhammad Khan brought cyberspace into a spectrum of 21st-century security. It helped the study to focus on different approaches necessary to shed light on the debate of international norms. Furthermore, this inquiry thanks Azher Mahmood on his timely response to review the drafts and help the study meet the subject matter's qualitative discourse.

References

Arquilla J & Ronfeldt DF (1997) In Athena's Camp: Preparing for Conflict in the Information Age. CA: Rand Corporation.

Bieda D & Halawi L (2015) Cyberspace: A venue for terrorism. Issues in Information Systems 16 (3):33-42.

Cavelty MD (2013) From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. International Studies Review 15 (1):105-122. https://doi.org/10.1111/misr.12023.

Clement J (2019) Worldwide digital population as of October 2019. [Accessed 9 June 2020]. https://www.statista.com/statistics/617136/digital-population-worldwide/.

Davis JA & Lewis C (2019) Beyond the United Nations Group of governmental experts. The Cyber Defense Review (2019):161-168.

Feaver P & Inboden W (2018) Washington needs a new solarium project to counter cyber threats. Foreign Policy, 26 June. [Accessed 9 May 2020]. https://foreignpolicy.com/2018/06/26/washington-needs-a-new-solarium-project-to-counter-cyberthreats/.

France Diplomacy (2019) France and cyber security. [Accessed 9 April 2020]. https://www.diplomatie.gouv.fr/en/french-foreign-policy/defence-security/cyber-security/.

Goel S (2020) National cyber security and the emergence of strong digital borders. Connections: The Quarterly Journal 19 (1):73-86. https://doi.org/10.11610/Connections.19.1.07.

Hayward RJ (2017) Evaluating the imminence of a cyber-attack for purposes of anticipatory self-defense. Columbia Law Review 117 (2):399-434.

Heickero R (2010) Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations. Stockholm: Defense Analysis, Swedish Defense Research Agency (FOI).

Jia K, Kenney M, Mattila J, & Seppala T (2018) The application of artificial intelligence at Chinese digital platform giants: Baidu, Alibaba and Tencent. ETLA Reports 81 (2018):1-11. https://doi.org/10.2139/ssrn.3154038.

Klimburg A (2020) Mixed signals: A flawed approach to cyber deterrence. Survival 62 (1):107-130. https://doi.org/10.1080/00396338.2020.1715071.

Koh HH (2012) International law in cyberspace. Harvard International Law Journal 54 (2012):1-12.

Lyndsey N (2019) US cyber command signals more aggressive approach involving persistent engagement ahead of 2020 election. [Accessed 10 March 2020]. https://www.cpomagazine.com/cyber-security/us-cyber-command-signals-more-aggressive-approach-involving-persistent-engagement-ahead-of-2020-election/.

Leuprecht C, Szeman J, & Skillicorn DB (2019) The damoclean sword of offensive cyber: Policy uncertainty and collective insecurity. Contemporary Security Policy 40 (3):382-407. https://doi.org/10.1080/13523260.2019.1590960.

Lynn III WJ (2010) Defending a new domain-the Pentagon's cyberstrategy. Foreign Affairs 89 (5):97-108.

Molander RC, Riddile AS, & Wilson PA (1996) Strategic Information Warfare: A New Face of War. CA: Rand Publisher.

Nakashima E (2018) Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes. The Washington Post, 13 January. [Accessed 9 June 2020]. https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

Nolan A (2015) Cybersecurity and Information Sharing: Legal Challenges and Solutions. Washington DC: Congressional Research Service.

North Atlantic Treaty Organization (2016) The Warsaw Declaration on Transatlantic Security: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016. [Accessed 5 June 2020]. https://www.nato.int/cps/en/natohq/official_texts_133168.htm.

Norton Cyber Security (2017) Norton cyber security insights report 2017 global results. [Accessed 5 June 2020]. https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf.

Pytlak A & Mitchell GE (2016) Power, Rivalry and Cyber Conflict: An Empirical Analysis. In: Karsten F & Jens R (eds). Conflict in Cyber Space: Theoretical, Strategic, and Legal Perspectives. London: Routledge.

Rosenberger L (2020) Making cyberspace safe for democracy: The new landscape of information competition. Foreign Affairs, May/June. [Accessed 6 June 2020] https://www.foreignaffairs.com/articles/china/2020-04-13/making-cyberspace-safe-democracy.

Rosenbach E & Chong SM (2019) Governing cyberspace: State Control vs. The Multistakeholder Model. In: Belfer Center for Science and International Affairs, Harvard Kennedy School, August.

Sanger DE (2018) Why hackers aren't afraid of us. The New York Times, 16 June. [Accessed 5 March 2020]. https://www.nytimes.com/2018/06/16/sunday-review/why-hackers-arent-afraid-of-us.html.

Schmitt MN (ed) (2013) Tallinn Manual on the International Law Applicable to Cyber Warfare. UK: Cambridge University Press.

Shaohui T (2017) International strategy of cooperation on cyberspace. Xinhua News, 1 March. [Accessed 1 April 2020]. http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm.

Shen Y (2016) Cyber sovereignty and the governance of global cyberspace. Chinese Political Science Review 1 (1):81-93. https://doi.org/10.1007/s41111-016-0002-6.

Singer PW & Friedman A (2014) Cybersecurity: What Everyone Needs to Know. UK: Oxford University Press.

Townsend K (2020) Analyzing cyberspace solarium commission's blueprint for a cybersecure nation. Security Week, 18 March. [Accessed 20 June 2020]. https://www.securityweek.com/analyzing-cyberspace-solarium-commissions-blueprint-cybersecure-nation.

U.S. Department of Defense (2016) All cyber mission force teams achieve initial operating capability. [Accessed 19 May 2020]. https://www.defense.gov/Explore/News/Article/Article/1524747/cyber-mission-force-achieves-full-operational-capability/.

Weinstein D (2014) Snowden and U.S. cyber power. Georgetown Journal of International Affairs 15 (2014):4-11.

White House (2017) Statement by President Donald J. Trump on the elevation of cyber command. [Accessed 2 March 2020]. https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/.