국제학석사학위논문

New Plane of US-Russia Rivalry:

An Analysis of Cyber Strategic Competition between the U.S. and Russia

신 미러 경쟁:

미국과 러시아 간의 사이버 전략 경쟁 분석

2018 년 8 월

서울대학교 국제대학원

국제학과 국제협력전공

김 시 령

Master's Thesis of International Studies

New Plane of US-Russia Rivalry:
An Analysis of Cyber Strategic Competition between the U.S. and Russia

신 미러 경쟁:
미국과 러시아 간의 사이버 전략 경쟁 분석

August 2018

Graduate School of International Studies
Seoul National University
International Cooperation Major

Si-Ryoung Kim

New Plane of US-Russia Rivalry:
An Analysis of Cyber Strategic Competition between the U.S. and Russia

신 미러 경쟁:
미국과 러시아 간의 사이버 전략 경쟁 분석

지도교수 신성호

이 논문을 국제학 석사학위논문으로 제출함

2018년 8월

서울대학교 국제대학원

국제학과 국제협력전공

김시령

김시령의 석사학위논문을 인준함

2018년 8월

위 원 장 김상배 (인)

부 위 원 장 한정훈 (인)

위 원 신성호 (인)

ABSTRACT

New Plane of US-Russia Rivalry: An Analysis of Cyber Strategic Competition between the U.S. and Russia

Si-Ryoung Kim
International Cooperation
Graduate School of International Studies
Seoul National University

This paper argues that the competition between the United States (US) and Russia in cyberspace is a hegemonic competition to achieve global dominance. Experts have stated that cyberwarfare is imminent and will be destructive than nuclear warfare if it happens. Thus, cyberwarfare needs to be prevented. Deterrence has been suggested as a means to prevent cyberwarfare since it has successfully prevented nuclear warfare. However, the unique nature of cyberspace makes deterrence ineffective. This failure has compelled states like the US and Russia to collaborate to find ways to prevent cyberwarfare. However, because there is not a universal understanding of cyber-norms, states understand, interpret and approach cyberspace differently.

The US seeks cybersecurity and the free flow of information while Russia seeks information security and state sovereignty in cyberspace. Thus, this paper argues that deterrence does not work to prevent conflict in cyberspace due to the unique nature of cyberspace – virtuality and anonymity – that are different from conventional domains. Because of the failure of deterrence, the US and Russia have sought alternative approaches to prevent conflict in cyberspace. However, this also failed due to fundamentally different perceptions of cyberspace. This has led the US and Russia to compete for hegemonic status in cyberspace to promote an international order that favors itself.

Keyword: Cybersecurity, Information Security, the United States, Russia, Competition, Cyberspace, Deterrence, Hegemony
Student Number: 2016-25471

TABLE OF CONTENTS

I. Introduction

1. Background

With the rapid technological development in the past few decades, the 21st century was marked as the digital information era. People gained more access to vast information and connected with others more easily, leading to more a globalized and interdependent world. Experts from Intel say that by 2020, the world will be connected with more than 200 billion technologies that are deeply integrated into everyday life.[1] Such technological progress has led to both positive and negative developments. Peoples' daily lives became more convenient, but this connectivity also led to the emergence of a new kind of threat that the world has not encountered before. With current technology, attacks against enemies can be conducted thousands of miles away without ever being physically involved. Banks can be robbed without ever entering the bank, and identities can be stolen without stealing a wallet.[2] Because of this, the complexity and the importance of cybersecurity have grown exponentially.

In November 2017, Microsoft president Brad Smith called for a Digital Geneva Convention with an emerging threat in the cyberspace during a speech

[1] Cesar Cerrudo, "Why Cybersecurity Should Be The Biggest Concern Of 2017," *Forbes*, January 17, 2017, https://www.forbes.com/sites/forbestechcouncil/2017/01/17/why-cybersecurity-should-be-the-biggest-concern-of-2017/..
[2] G. Alexander Crowther, "National Defense and the Cyber Domain," *The Heritage Foundation*, October 5, 2017, 83–97.

at the United Nations in Geneva.[3] Smith stated that history taught the world that war could not be prevented on land, maritime, air and space "unless there were international rules to govern… [and] we now live in an age that requires established rules for cyberspace as well."[4] Thus, Smith argued that the world needs a Digital Geneva Convention where all nations need to come together to establish and adopt policies to prevent such an attack in cyberspace, and future cyberwarfare that could be more destructive than nuclear warfare.[5]

According to Joseph Nye, cyberspace is a domain that includes the "[i]nternet of network computers but also intranets, cellular technologies, fiber optic cables, and space based communications."[6] In this sense, cybersecurity refers to "a state's ability to protect itself and its institutions against threats. espionage, sabotage, crime and fraud, identify theft and other destructive e-interactions and e-transaction."[7] Simply put, cyberspace includes various Information Communication Technology (ICT) systems that protect a state's content from cyberattacks. Recently, cyberattacks—hostile actions in cyberspace—have evolved from individual identity theft to the penetration of

[3]Dustin Volz, "Microsoft President Brad Smith Calls for a 'Digital Geneva Convention' in the Wake of the DNC Hacking Scandal," *Business Insider*, February 14, 2017, http://www.businessinsider.com/r-digital-geneva-convention-needed-to-deter-nation-state-hacking-microsoft-president-2017-2.)
[4] Ibid.
[5] Bradley Blakeman, "Cyber Warfare More Dire and Likely than Nuclear," The Hill, 27 2016, http://thehill.com/blogs/pundits-blog/technology/281475-cyber-warfare-more-dire-and-likely-than-nuclear.
[6] Joseph S. Nye, "Nuclear Lessons for Cyber Security:" (Fort Belvoir, VA: Defense Technical Information Center, January 1, 2011), https://doi.org/10.21236/ADA553620
[7] Nazli Choucri, *Cyberpolitics in International Relations* (MIT Press, 2012).

government Internet Technology (IT) infrastructure. These threats do not just come from state actors. They now also come from non-state actors such as private companies or individuals. Cyberattacks have been increasingly prevalent in the past few years. Cyberspace is now considered as a new arena by the international community. The paradigm of cyberspace and cybersecurity has shifted from internet and privacy security to the top national threat that could risk national security.[8] However, cyberspace has no established rule of engagement and limitations to control such threats, which ultimately led to strategic competition among states.

In the past, when states conducted war against each other, they used tangible tools such as swords, guns, missiles or nuclear weapons to physically attack or threaten their enemies. When states needed to extract pertinent information on the enemies' national security, they spied on their enemies using human agents. Now, all of this can be done with a simple click from miles away with a single malware using strings of computer codes.[9] Old rivalries, like that of the United States (US) vs. the Soviet Union (USSR) since the Cold War, have entered a new phase of "war by other means": cyber. Furthermore, in the conventional arenas, states were able to prevent war by strategically achieving deterrence where a state would deter a potential adversary's attack by imposing

[8] Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, Reprint edition (New York: Ecco, 2011).
[9] Crowther, "National Defense and the Cyber Domain," 83

high expected costs in return. However, in cyberspace, this is nearly impossible because the damage inflicted by a cyberattack is unlike that resulting from a conventional attack where the attackers, destruction of buildings, and casualties are all visible.[10]

With rising threats posed in cyberspace, the US and Russia have engaged in numerous dialogues and issued various joint statements highlighting mutual understanding and collaboration in cyberspace to prevent crises. However, despite these efforts to cooperate on cybersecurity, the fundamental differences between the US and Russia in their recognition of and approach towards cyberspace and cybersecurity have made bilateral cooperation hardly possible; rather, these differences led to them to compete for dominance.[11] The US and Russia have a long history of cooperative-competitive relationship to attain dominance and be a hegemonic power on a different battleground. This relationship eventually led to the rivalry that was clearly shown in the Cold War: the strategic nuclear competition, which was the biggest rivalry in history.[12] Given this history, the nature of the US and Russia's competition in cyberspace is also to become the dominant power, particularly through controlling

[10] Longdi Xu, "Cyberspace Security: Trends, Conflicts and Strategic Stability" (China Institute of Internaitonal Studies, November 10, 2017), http://www.ciis.org.cn/english/2017-11/10/content_40064730.htm.
[11] Bruce W McConnell, Pavel Sharikov, and Maria Smekalova, "Suggestions on Russia-U.S. Cooperation in Cybersecurity" (Russian International Affairs Council and EastWest Institute, May 11, 2017), http://russiancouncil.ru/en/activity/policybriefs/suggestions-on-russia-u-s-cooperation-in-cybersecurity/.
[12] Godfried van Benthem van den Bergh, "The Taming of the Great Nuclear Powers," *Carnegie Endowment for International Peace*, 2009, 20.

international rules on internet governance and norms that have not yet been agreed upon by the international community. One cannot deny that the US currently holds hegemony in cyberspace with its advanced information technology, but Russia is continuously trying to develop an international rule that favors and stabilizes Russian state sovereignty.[13]

The US and Russia's competition in cyberspace is fierce and ongoing, and they seek to undermine the global order to gain more advantage. However, this strategic competition between the US and Russia in cyberspace takes a different form from that of nuclear competition in the Cold War. During the Cold War, both the US and Russia had a shared understanding of nuclear warfare. They both knew what would happen in the event of nuclear war, and they possessed weapons of similar technological sophistication. However, in cyber, these two states have a different understanding of cyberspace and cybersecurity. The Russian government does not use the term "cybersecurity" in their doctrine. They use "information security" to justify state sovereignty in cyberspace. [14]

Furthermore, unlike the nuclear competition where both competitors have to be fairly advanced in their technology to pose a threat, in cyber, that is less likely so. For example, one cannot deny that the US is the most advanced

[13] Julien Nocetti, "Contest and Conquest: Russia and Global Internet Governance," *International Affairs* 91, no. 1 (January 2015): 111–30, https://doi.org/10.1111/1468-2346.12189.
[14] Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," CNA's Occasional Paper (CNA Analysis & Solution, March 2017), https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf.

country with its IT and technologies, but when the US speaks of its competitors, countries like Iran and North Korea are also included as rising competitor in cyberspace even though they are not considered to be not as advanced as the US.[15] Thus, while the nuclear competition was characterized by a shared understanding and similar level of technological progress that made deterrence possible, the US-Russia competition in cyberspace is taking a different path. This unique characteristics of cyberspace and absence of shared international norms prevent deterrence, leading to a struggle for hegemony[16]

With the dramatic advancement of technology and corresponding growth in interdependence between the military and IT, cyberspace has left the realm of a purely "virtual reality." It has taken on a characteristic of actual real space that can be "invaded" like a real territory. However, as aforementioned, the history of the internet is relatively short; cybersecurity is also a young phenomenon with few cases to learn from. On the other hand, the US and Russia have built a substantial early history in this new arena for strategic competition. Understanding how and why the US and Russia have begun and developed their competition in cyberspace can be beneficial for obtaining further insights into how the future of competition in cyberspace may be prevented and deterred, as this competition could ultimately lead to

[15] Crowther, "National Defense and the Cyber Domain," 87
[16] Clorinda Trujillo, "The Limits of Cyberspace Deterrence," *National Defense University Press* Joint Force Quarterly, no. 75 (2014): 10.

cyberwarfare that is more dire and deadly than conventional warfare.[17]

This paper argues that deterrence has failed in cyberspace due to its unique nature and this failure has led states to come together to search for different ways to prevent possible conflicts. However, cooperation ultimately failed due to different perceptions and understandings that disabled states from cooperating, leading to a hegemonic competition in cyberspace. In the case of the US and Russia, because the US favors free flow of information and Russia favors state control in cyberspace, the two states have failed to come to an agreement even though they have tried to collaborate.

Hence, this paper will first examine the concept of deterrence to discuss the characteristics of deterrence in the conventional arenas, particularly during the Cold War with nuclear weapons, and then explain why deterrence does not work in cyberspace. It will then look into the notion of cybersecurity and information security to clarify the different approaches that the US and Russia are taking in cyberspace. The second will explore the US and Russia's competition in cyberspace in four areas: cyber strategy, including current security policies; militarization of cyberspace; competition in standardization; and Russian interference in the 2016 US election. This section will demonstrate the differences between these two states in their policies, norms, and regulations

[17] Blakeman, "Cyber Warfare More Dire and Likely than Nuclear."; Ellyne Phneah, "Cyber Warfare Not Theoretical, Can Actually Kill," *ZDNet*, November 17, 2011, https://www.zdnet.com/article/cyber-warfare-not-theoretical-can-actually-kill/.

of cyberspace. It will then provide an overall analysis of the US-Russia competition in cyberspace. The paper will conclude by discussing the implications of the above analysis.

II. Deterrence and Cyberspace

1. Deterrence in Cold War

According to the Merriam-Webster Dictionary, deterrence means "the act or process of deterring: such as… the maintenance of military power for the purpose of discouraging attack."[18] Even though deterrence theory gained prominence as a key military strategy during the Cold War, the idea of deterrence predates the nuclear competition between the US and the USSR.[19] Conventional deterrence was achieved by denial; the whole concept was to deny the aggressor's prospect of easy victory at a reasonable cost.[20] "Reasonable cost" meant building up a large army, fortress or wall that would make opponents believe they would not win if they were to attack. Thus, the aggressors will be deterred from attacking in the first place.[21]

However, this basic idea of deterrence evolved with the development of nuclear weapons. The destructive power of nuclear weapons overshadowed the concept of defensive deterrence by denial (conventional deterrence) to offensive deterrence by punishment (nuclear deterrence), more specifically by

[18] "Deterrence," *Merriam-Webster Dictionary*, July 3, 2018, https://www.merriam-webster.com/dictionary/deterrence.
[19] John Harvey, *Conventional Deterrence and National Security* (Fairbairn, A.C.T.: Air Power Studies Centre, 1997).
[20] Michael S. Gerson, "Conventional Deterrence in the Second Nuclear Age:" (Fort Belvoir, VA: Defense Technical Information Center, October 1, 2009), https://doi.org/10.21236/ADA510428.; Gary L Guertner, Robert Haffa, and Geroge Quester, "Conventional Forces and the Future of Deterrence," *Strategic Studies Institute, U.S. Army War College*, Strategic Concepts in National Military Strategy, March 5, 1992, 68.
[21] Gerson, "Conventional Deterrence in the Second Nuclear Age," 43

the threat of inflicting unacceptable damage or complete destruction on the aggressors if they were to attack the opponent.[22] During the Cold War, nuclear deterrence became a critical military strategy when the USSR developed nuclear weapons, thereby ending the US monopoly. The US faced the increasing "prospect of the same fate it had held out for its enemies"[23] as both states achieved deterrence through the use of increasingly large stockpiles of nuclear weapons.

In the early part of Cold War, both sides had nuclear weapons but only one method—bombers—to deliver them. Nuclear deterrence policy was not enhanced until both states developed additional delivery systems. By the middle of the Cold War, the US and USSR developed different kinds of delivery systems and nuclear weapons. The whole idea of nuclear deterrence was that if one side attacks with nuclear weapons, that attack will be met with a retaliatory response from the other side which would result in the destruction of both sides. This idea became widely known as Mutually Assured Destruction or MAD.[24] Because both states had sufficient capabilities to ensure MAD, they were in a mutual hostage situation where the balance of terror and fear would prevent

[22] Robert Powell, "Nuclear Deterrence Theory, Nuclear Proliferation, and National Missile Defense," *International Security* 27, no. 4 (April 2003): 86–118, https://doi.org/10.1162/016228803321951108.
[23] Carl H. Builder, "The Future of Nuclear Deterrence" (Santa Monica: RAND Corporation, 1991), https://www.rand.org/pubs/papers/P7702.html
[24] Kenneth N. Waltz, "Nuclear Myths and Political Realities," *The American Political Science Review* 84, no. 3 (September 1990): 731, https://doi.org/10.2307/1962764.

nuclear warfare.[25]

As cyberspace has been recognized as a fifth domain following land, maritime, air and space, it is essential to discuss and study what cyberspace is to understand why deterrence has failed in this domain. There are recent studies on cyber deterrence: whether deterrence is possible in cyberspace. While some say that the deterrence is possible in cyberspace under multiple sets of conditions, most scholars agree that deterrence is not possible in cyberspace.[26] The US government tried to implement a retaliatory policy in cyberspace "to deter and defeat aggression," and it also attempted to jointly operate deterrence policy with different nations such as Russia.[27] Despite states' effort to establish an international order in cyberspace, the failure to do so has led to a strategic competition between states to achieve hegemony in cyberspace.[28]

2. What is Cyberspace?

Because cyberspace and cybersecurity have a relatively short history compared to other domains, there is relatively little research on this new arena. In a review of relevant articles and policy papers published between 2001 and

[25] Gerson, "Conventional Deterrence in the Second Nuclear Age," 36
[26] Patrick Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, 2010, https://doi.org/10.17226/12997; Sean Lyngaas, "Intel Chiefs Say Cyber Norms, Deterrence Strategy Still Elusive," *FCW*, September 10, 2015, https://fcw.com/articles/2015/09/10/intel-cyber-norms.aspx.
[27] Trujillo, "The Limits of Cyberspace Deterrence," 46
[28] Alexandra Kulikova, "The Contest of Rules: US, China, Russia Rival in Setting the Norms of Behavior in Cyberspace," *Center for Global Communication Studies Mediawire* (blog), October 8, 2015, https://global.asc.upenn.edu/the-contest-of-rules-us-china-russia-rival-in-setting-the-norms-of-behavior-in-cyberspace/.

2010, Brandon Reardon and Nazli Choucri examine four theoretical approaches: realism, liberalism, and constructivism. [29] According to Reardon and Choucri, realists viewed whether the cyber technology will become a new source of conflict or peace and whether states will participate in the cyber arms race. They argue that the development and growth of cyberspace undermine the authority of the state and empower new international actors. Liberals explained how cyberspace can promote the development and diffusion of political thought, the organization of civil society, and the development of multinational social networks, and how access and control of cyberspace can shape national behavior and influence international politics. Liberal institutionalism stated that international cooperation could be applied to issues related to cybersecurity, cyberspace governance, and cyber arms control. Finally, Reardon and Chourci found that constructivists dominate the academic literature on cyber conflict. Constructivists focus on the way that cyberspace enables the spread of information that could change the perceptions that could threaten the existing social order, and ultimately national security.[30]

Many studies of cyberspace and cybersecurity have highlighted the grave damage that cyber conflicts could cause.[31] As fear and perception can become

[29] Robert Reardon and Nazli Choucri, "The Role of Cyberspace in International Relations: A View of the Literature," vol. 1 (ISA Annual Convention, San Diego, 2012), 34.
[30] Ibid.
[31] Choucri, *Cyberpolitics in International Relations*; Clarke and Knake, *Cyber War*; Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38, no. 2 (October 2013): 7–40, https://doi.org/10.1162/ISEC_a_00138.

a powerful force for security competition, cyber threats are currently being addressed as the most significant problem of national security. According to traditional armaments competition theory, fear and perception can be a much more powerful force in security competition than real threats.[32] Cyberspace can cause potential risk to countries' infrastructures as these systems depend on Internet networks in cyberspace, which is basically all of the computer networks in the world as well as everything they connect and control.[33] Furthermore, the development of cyberspace has put countries in an 'unprecedented situation' characterized "by high levels of uncertainty as they try to maintain control in the face of a changing global security environment."[34]

Then, what is the notion and meaning of cyberspace in the 21st century? As aforementioned, cyberspace has been accepted as a battlefield (as an "operational domain") by the members of the North Atlantic Treaty Organization (NATO) at their 2016 summit. They also emphasized strengthening the cyber defense capabilities of each country and co-operation between countries.[35] However, there still is no international consensus on what cyberspace is; F. D. Kramer stated that there are 28 different definitions of the

[32] A. Craig and B. Valeriano, "Conceptualising Cyber Arms Races," in *2016 8th International Conference on Cyber Conflict (CyCon)*, 2016, 141–58, https://doi.org/10.1109/CYCON.2016.7529432.
[33] Nye, "Nuclear Lessons for Cyber Security."; Clarke and Knake, *Cyber War*;
[34] Choucri, *Cyberpolitics in International Relations*; Craig and Valeriano, "Conceptualising Cyber Arms Races."
[35] Doug G. Ware, "NATO Officially Recognizes Cyberspace as Domain for War," *UPI*, June 14, 2016, https://www.upi.com/NATO-officially-recognizes-cyberspace-as-domain-for-war/2271465941545/.

term.[36] According to the US *Department of Defense Dictionary of Military and Associated Terms*, cyberspace is defined it as a "global domain within the information environment consisting of the interdependent network of information technology infrastructure, including the Internet, telecommunications networks, computer systems and embedded processor and controllers." [37] The Russian government, in its *Concept Strategy of Cybersecurity of the Russian Federation*, defined it as "a sphere of activity within the information space, formed by a set of communication channels of the internet and other telecommunications networks, the technological infrastructure to ensure their functioning, and any form human activity on them." [38] However, even though there is not an established definition of cyberspace, it can be broadly understood as a telecommunication space created by the worldwide interconnection of automated digital data processing technology and is made up of digital networks that are used to store, modify and communicate information.[39]

The two primary characteristics that separate cyberspace from the conventional domains are virtuality and anonymity. Telecommunication networks allow people to interact far beyond their geographical or physical

[36] Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds., *Cyberpower and National Security* (University of Nebraska Press, 2009), http://www.jstor.org/stable/j.ctt1djmhj1.
[37] Tim Maurer and Robert Morgus, "Compilation of Existing Cybersecurity and Information Security Related Definitions" (New America Foundation, October 2014).
[38] Ibid.
[39] Ibid.

location. This means that there is no physical limitation in cyberspace where a state can claim its authority and jurisdiction in a certain location, unlike in conventional domains.[40] Also, this virtual domain takes no physical form, and aggressors do not need to deploy physical forces or gain physical access to a region.[41] Physical boundaries on land indicate which state has authority over a given region. In space, there are different sectors to ensure that satellites' orbits do not overlap with each other.[42] In cyberspace, none of these exist. Instead, it is an interconnected domain where the state and non-state actors can all intertwine, and any operations can be fully automated without limitation.

The immediate damage resulting from a cyberattack is hard to detect, as it is a virtual space. Of course, various systems and computers can be destroyed. However, unlike conventional arenas where one could see damages such as casualties caused by conventional weapons, it is harder or nearly impossible to recognize such damages due to the virtuality of cyberspace. Furthermore, because the domain is virtual, cyberspace does not have a limitation in size. It is continuously expanding and evolving as every action by an actor can bring subtle changes to the domain.[43] This is significantly different from the fixed and

[40] Crowther, "National Defense and the Cyber Domain."
[41] Ibid.
[42] David R. Johnson and David G. Post, "Law and Borders - the Rise of Law in Cyberspace," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, February 1, 1997), https://papers.ssrn.com/abstract=535.
[43] David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (Routledge, 2004), https://doi.org/10.4324/9780203508176.

physical nature of the other domains.[44]

Anonymity is another characteristic that sets cyberspace apart from the conventional domains. Anonymity is a state of being unknown to most other people. Due to the nature of the technology that "enables anyone to communicate…to hundreds or thousands of other people, nearly instantaneously" and share ideas over great distances free from geographic and physical constraints, cyberspace makes it easier to acquire anonymity.[45] Anonymity makes it harder to identify the aggressor when a crime or attack has occurred, unlike the conventional domains where the aggressor is usually visible and identifiable. Further, if the aggressor cannot be clearly identified, there is no validity and credibility to claims about who is responsible for an attack.[46] Before cyberspace existed, having truly anonymous communication was much more laborious and time-consuming. An anonymous letter had to be careful without any traceable fingerprints or materials such as regional dirt, paper, and ink. An anonymous call had to be short or use an untraceable pay phone, and voices had to be digitally altered to avoid identification.[47] In cyberspace, people can send an anonymous email by creating an account without using their real identities. The geological location can be hidden by

[44] "What Is Cyberspace? Examining Tts Characteristics," *Air Power Development Centre* Pathfinder, no. 157 (June 2011).
[45] George du Pont, "Criminalization of True Anonymity in Cyberspace, The," *Michigan Telecommunications and Technology Law Review* 7, no. 1 (2011): 27.
[46] Trujillo, "The Limits of Cyberspace Deterrence."
[47] du Pont, "Criminalization of True Anonymity in Cyberspace, The.".

using a proxy server or different Internet Protocol (IP) addresses. The voice alteration program is now far more sophisticated, and people can access these programs more easily and at a lower cost than before.[48]

Because of these two unique characteristics of virtuality and anonymity, it is hardly possible to apply deterrence in cyberspace. During the nuclear competition in the Cold War, the development of nuclear weapons was a mutual military buildup. There was a mutual understanding of MAD between the US and Russia, and similarly advanced technology on both sides made deterrence possible.[49] However, in cyberspace, this is nearly impossible because its domain is virtual and the aggressor is anonymous or harder to detect. The level of technology does not have to be advanced to launch an attack. In fact, many experts argue that the more advanced the state is, the more vulnerable it is to cyber threats and cyber attacks.[50] Because states cannot deter or deviate from a possible attack, the US and Russia were compelled to find different ways to jointly manage cyberspace. However, efforts to cooperate ultimately failed because of the different perceptions they have of cyberspace, leading them to compete against each other in cyberspace to obtain the state's safety through its hegemony. This paper will show the US-Russia hegemonic competition

[48] Ionela Maria Ciolan, "Defining Cybersecurity as the Security Issue of the Twenty First Century. A Constructivist Approach," *The Public Administration and Social Policies Review* 5, no. 1 (2014): 17.
[49] Gerson, "Conventional Deterrence in the Second Nuclear Age."
[50] Kellie Ell, "FireEye CEO: If the US and Russia Had a Cyber War, Russia Would Win," March 15, 2018, https://www.cnbc.com/2018/03/15/fireeye-ceo-if-the-us-and-russia-had-a-cyber-war-russia-would-win.html.

happening in cyberspace due to the different perceptions the two states have.

3. Cybersecurity vs. Information Security

The most important aspect of US-Russia competition is the difference in each country's perception of security in cyberspace. The US uses the term, 'cybersecurity' whereas Russia uses 'information security.'[51] The two terms 'cyber-security' and 'information-security' ultimately mean the same: protecting the network system in cyberspace.[52] However, states and experts use these two terms in very different ways.

Information security is a broader field that concerns the information and the protection of information whether it is in cyberspace or other domains. In that sense, information security is "the protection of information and its systems from unauthorized access, use, disclosure, modification or destruction"[53] of information regardless of realm. Information security is a condition of security of its national interests in the informational space, determined by a balanced combination of the interests of the individual, society, and the state.[54] Thus, the

[51] Maurer and Morgus, "Compilation of Existing Cybersecurity and Information Security Related Definitions."
[52] Melissa Stevens, "Cybersecurity Vs. Information Security: Is There A Difference?," *BitSight* (blog), March 15, 2016, https://www.bitsighttech.com/blog/cybersecurity-vs-information-security.
[53] Definition of Information security from "United States Code, 2006 Edition, Supplement 5, Title 44 - PUBLIC PRINTING AND DOCUMENTS"
[54] Stevens, "Cybersecurity Vs. Information Security."; Aniruddha Singh, Abhishek Vaish, and Pankaj Kumar Keserwani, "Information Security: Components and Techniques," *International Journal of Advanced Research in Computer Science and Software Engineering* 4, no. 1 (2014): 6.

problem of information security involves "not only the risks arising from the weakness of the basic information infrastructure but also the political, economic, military, social, cultural and numerous other types of problems created by the misuse of information technology."[55]

Cybersecurity, on the other hand, only deals with the protection of cyberspace.[56] According to the U.S. Department of Commerce, cybersecurity is "the ability to protect or defend the use of cyberspace from cyberattack"[57] It is also about the security network system that is vulnerable through ICT. Cybersecurity does not deal with information in paper form and only deals with threats against cyberspace. It strives against cybercrime, cyber fraud, and law enforcement. It is only about the protection of digital information.[58] In this sense, cybersecurity is considered to be a subset of information security.[59]

These differences also led to different perceptions of security in cyberspace between the US and Russia, which became the fundamental reason for the current US and Russian competition in cyberspace.

---

[55] Ibid.
[56] "Cyber Security Vs Information Security," *Hack2Secure* (blog), June 16, 2017, https://www.hack2secure.com/blogs/cyber-security-vs-information-security.; Ray Klump, "Information Assurance vs. Cyber Security vs. Information Security: Clarifying the Differences | Faculty Forum," *Lewis University Faculty Forum* (blog), January 6, 2018, https://www.lewisu.edu/experts/wordpress/index.php/information-assurance-vs-cyber-security-vs-information-security-clarifying-the-differences/.
[57] Richard Kissel, "Glossary of Key Information Security Terms" (National Institute of Standards and Technology, May 2013), https://doi.org/10.6028/NIST.IR.7298r2.
[58] Stevens, "Cybersecurity Vs. Information Security."
[59] Ibid

III. The US and Russia's Cyber Competition

According to Tsuyoshi Kawasaki, strategic competition is a power struggle over a particular international "political order on the question of who governs this order."[60] It is a 'tug of war' between the hegemonic state's desire to stay in power and challenging state's intention to change that international order.[61] This kind of inter-state power struggle has a political aspect with its concern for the governance of international political order such as global norms and regulations. States "resort to a wide range of policy instruments including politico-diplomatic, military, economic, and cultural… [and] also engage in covert and intelligence activities within their competitors' domestic spheres."[62] In order to maintain or alter the power balance, the hegemonic and challenging states usually struggle over the elements of the existing global order such as territorial arrangements, international rules, and ideologies.[63] This kind of competition between the US as the hegemonic power and Russia as a challenger that is currently playing out in cyberspace.

Because there is not a clear consensus on cyberspace, and there are a wide range of threats such as individual identity theft to government infrastructure penetration that are present in cyberspace, scholars have been

[60] Tsuyoshi Kawasaki, "Where Does Canada Fit in the US–China Strategic Competition across the Pacific?," *International Journal* 71, no. 2 (June 1, 2016): 214–30, https://doi.org/10.1177/0020702016643344.
[61] Ibid.
[62] Ibid, 217.
[63] Ibid

discussing the danger of cyberspace.[64] However, the cyber threat was not perceived as a problem of security until the start of the Distributed Denial of Service (DDoS) offensive against Estonia in 2007, which was the very first kind of cyberattack that penetrated a government system.[65] The Estonian incident, where major institutions such government agencies and banks were paralyzed, shocked the international community as it caused similar damages as those using conventional weapons. The Estonian government has alleged the Russian Federation's Security Service (FSB)[66] as the source of the cyber attack, but since there has not been any credible evidence, the allegation was not carried further. This incident stunned the international community and raised awareness of the cyber threat and the need to increase national security in cyberspace.[67]

To prevent such an attack from happening in the first place, the US and Russia tried to cooperate in the realm of security. In 1998, the US and Russia had their first declaration of mutual interests in cooperation on the international response to cybersecurity threats.[68] The US and Russia engaged in dialogue in 2011 and issued a joint statement, which was signed by Cybersecurity

[64] Clarke and Knake, *Cyber War*.
[65] 성기노, 「세계 최초의 사이버 전쟁과 사이버안보법」. 『*보안뉴스*』, February 5, 2017, http://www.boannews.com/media/view.asp?idx=53325.
[66] From its name in Russian: Federal'naya sluzhba bezopasnosti
[67] 성기노, 「세계 최초의 사이버 전쟁과 사이버안보법」
[68] Franz-Stefan Gady and Greg Austin, "Russia, The United States, And Cyber Diplomacy: Opening the Doors" (EastWest Institute, 2010).

Coordinator for the Obama Administration Howard Schmidt and Deputy Secretary of the Security Council Nikolai Klimashin, on cybersecurity that highlighted "mutual understanding on national security issues in cyberspace… facilitates better collaboration in responding to cyberthreats."[69] Furthermore, during the 2013 G8 summit, the US and Russia issued another joint statement, "Joint Statement by the President of the United States of America and the Russian Federation on a New Field of Cooperation in Confidence Building" on cybersecurity. [70] President Obama and President Putin agreed to create a mechanism "to facilitate the regular exchange of practical technical information on cybersecurity risk to the critical system" and authorized a "direct secure voice communication line [hot line] between the U.S. Cybersecurity Coordinator and the Russian Deputy Secretary of the Security Council… to directly manage a crisis situation arising from an ICT security incident" to strengthen bilateral relations in cyberspace.[71]

However, former US Central Intelligence Agency (CIA) employee Edward Snowden's WikiLeaks in 2013, as well as Russian intervention in

[69] Joint Statement by Cybersecurity Coordinator Schmidt and Deputy Secretary Klimashin, Washington, DC, June 23, 2011; Eric Chabrow, "Schmidt Meets with Russian Counterpart," July 2011, https://www.govinfosecurity.com/schmidt-meets-russian-counterpart-a-3841.
[70] The White House, "FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security," whitehouse.gov, June 17, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol.
[71] Sean Gallagher, "US, Russia to Install 'Cyber-Hotline' to Prevent Accidental Cyberwar," *Ars Technica*, June 18, 2013, https://arstechnica.com/information-technology/2013/06/us-russia-to-install-cyber-hotline-to-prevent-accidental-cyberwar/.

Crimea and Donbass regions of Ukraine in early 2014, soon turned two states' cooperative stage into a continued confrontational stage. Snowden copied and leaked classified information from the US National Security Agency (NSA) that revealed PRISM. PRISM is a codename for the global surveillance program in which NSA collected internet communications from various US internet companies such as Facebook, Microsoft and Google Inc.[72] From Snowden's WikiLeaks on the US-run global surveillance program, the US received a lot of criticism from countries like Germany, Russia, and China because the US has been spying on both its rivals and allies.[73] A Russian official stated that US spying on Russian confidential communication would further hurt the US-Russia relationship.[74] However, the downfall of the US-Russia relationship actually began when Russia granted Snowden asylum.[75] Obama was furious with Putin's decision and canceled a presidential summit with Putin when Russia refused to return Snowden to the US. Obama further expressed his disappointment during an interview on NBC's Tonight Show by saying that

[72] T. C. Sottek, "Everything You Need to Know about PRISM," The Verge, July 17, 2013, https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet.
[73] "China Asks U.S. to Explain Internet Surveillance," *Reuters*, June 17, 2013, https://www.reuters.com/article/us-usa-security-china/china-asks-u-s-to-explain-internet-surveillance-idUSBRE95G06R20130617.; Matthew Karnitschnig, "NSA Flap Strains Ties With Europe," *Wall Street Journal*, February 9, 2014, sec. World, https://www.wsj.com/articles/wave-of-nsa-reports-strain-ties-with-europe-1391971428.
[74] Julian Borger, Luke Harding, and Miriam Elder David Smith in Johannesburg, "G20 Summits: Russia and Turkey React with Fury to Spying Revelations," *The Guardian*, June 17, 2013, sec. World news, http://www.theguardian.com/world/2013/jun/17/turkey-russia-g20-spying-gchq.
[75] Pavel Sharikov, "U.S.-Russia Relations in the Sphere of Information Security," Carnegie Moscow Center, November 1, 2013, https://carnegie.ru/2013/11/01/u.s.-russia-relations-in-sphere-of-information-security-pub-63163.

"[t]here have been times where [Russia] slip back into cold war thinking and a cold war mentality," in which Russian Nationalist Duma deputy Vladimir Zhirinovsky responded that Obama's action was disrespectful towards Russia.[76]

The already struggling US-Russia relations worsened when Crimea was invaded by pro-Russian separatist militia backed by the Russian government. After the Ukraine revolution and fall of President Viktor Yanukovych in early 2014, pro-separatists took over Crimea. A referendum on the issue of reunification with Russia was held following the seizure, and with a result favoring reunification, Russia annexed Crimea. Following the annexation, pro-separatists in Donbass protested against the Ukrainian government, and this escalated into an armed conflict between the Ukrainian government and pro-separatist forces. The US reacted strongly to Russia's intervention in Ukraine. During a press conference, Obama stated that Russia's actions are leaving Russia isolated from the international community and the US and its allies will increase economic sanctions to pressure Russia to leave Ukraine.[77]

There was a slight shift in relations towards cooperation when President Donald Trump, favored by Putin, took office in 2017. In July 2017, Trump mentioned the prospect of a joint working group called the 'Cyber Security Unit'

[76] Alec Luhn and Dan Roberts, "Obama Cancels Meeting with Putin over Snowden Asylum Tensions," *The Guardian*, August 7, 2013, sec. US news, http://www.theguardian.com/world/2013/aug/07/obama-putin-talks-canceled-snowden.
[77] "Ukraine Crisis: Obama Rules out Military Action," *The Associated Press*, August 28, 2014, https://www.cbc.ca/news/world/ukraine-crisis-obama-rules-out-military-action-1.2749066.

with Russia. This joint cyber unit was intended to address issues such as the risk of cyber interference in elections to "make sure that there was absolutely no interference whatsoever, that [Trump and Putin] would work on cybersecurity together."[78] The plan was retracted after receiving harsh criticism from the US politicians like Senator Lindsey Graham, who said that a joint cybersecurity unit was "not the dumbest idea… but it's pretty close."[79] In fact, tensions between the US (excluding Trump) and Russia spiked once again as Russia has been accused of interfering with the 2016 election.[80] Moreover, in 2018, there was an allegation that Russia had manipulated the regional voting machines during the 2016 election. Russia has denied all accusations about its involvement in any US election-related hacks or leaks.[81] However, tensions between the two countries have not cooled down, and cooperation between the US and Russia on cybersecurity has been put into question. Furthermore, with increasing concern and fear of cyberterrorism and warfare as well as the awareness of a new arms race, experts have predicted that it is only a matter of time before interactions in cyberspace turn towards more aggressive methods

[78] Phil Stewart and Valerie Volcovici, "Trump Backtracks on Cyber Unit with Russia after Harsh Criticism," *Reuters*, July 9, 2017, https://www.reuters.com/article/us-usa-trump-russia-cyber/trump-backtracks-on-cyber-unit-with-russia-after-harsh-criticism-idUSKBN19U0P4.
[79] Ibid.
[80] Joint statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security (DHS)
[81] Thomas Rid, "All Signs Point to Russia Being Behind the DNC Hack," Motherboard, July 25, 2016, https://motherboard.vice.com/en_us/article/4xa5g9/all-signs-point-to-russia-being-behind-the-dnc-hack.

of competing for the development of new kinds of cyber weapons.[82] With increasing threats in cyberspace, why do the US and Russia continue to fail to cooperate on an international agreement on cybersecurity?

The US government's notion of "cybersecurity" implies a technological understanding where the "primary goal of cybersecurity is to keep technologies safe from disruption, unauthorized access, or other kinds of interference,"[83] whereas the Russian government's notion of "information security" implies a political understanding where it protects national interests by "preventing political, economic, and social security threats emerging in cyberspace."[84] While the US policy on cyberspace highlights the free flow of information, Russia promotes global internet governance which emphasizes 'the element of sovereignty.'[85] Russia strives to take the lead in global cyber governance and security mainly because Russia does not agree with the US-centric consensus on cyber governance. Thus, it emphasizes its challenge to US dominance in the cyber domain and attempts to shift from US-centric cyber policy on the current international internet governance regime.[86]

---

[82] Christopher Bronk and Dan Wallach, "Cyber Arms Control? Forget about It," *CNN*, March 26, 2013, International Edition, https://edition.cnn.com/2013/03/26/opinion/bronk-wallach-cyberwar/index.html.
[83] Pasha Sharikov, "Cybersecurity in Russian-U.S. Relations," CISSM Policy Brief (Center for International Security Studies at Maryland, April 2013), http://www.cissm.umd.edu/publications/cybersecurity-russian-us-relations-0.
[84] Maurer and Morgus, "Compilation of Existing Cybersecurity and Information Security Related Definitions."
[85] 신범식, 「러시아의 사이버 안보의 전략과 외교」" in 『사이버 안보의 국가전략: 국제정치학의 시각』, 5 (서울: 사회평론아카데미, 2017), 397.
[86] Nocetti, "Contest and Conquest."

1. The US and Russia's Cyber Strategy

The US Strategy: Free Flow of Information

The US government has worked hard to promote free exchange and free access of information, a guarantee of the individual right of free expression, information, and open cyberspace, and it also developed defensive measures to protect its government infrastructure.[87] The US perception of cybersecurity is best reflected in the speech made in January 2010 by former Secretary of State Hillary Clinton. Clinton specifically addressed that the free flow of information through the Internet has a positive effect of promoting democracy and that the governments of other nations should not impose severe restriction on the Internet to achieve more democratic society.[88] Clinton also firmly stated that the US does not agree with some nations that are building a virtual wall to prevent the Internet from providing extensive knowledge for people and a potential market for businesses. [89]

The US already has a dominant influence over cyberspace and has a desire to maintain its hegemony.[90] To maintain its status, the US government pursues various policies in the domestic and international arena. In 2003, the Bush administration revealed the first systematic attempt to solve the national

[87] Kramer et al. *Cyberpower and National Security*.
[88] "Hillary Clinton's Historic Speech on Global Internet Freedom" (January 2010), //2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.
[89] Ibid.
[90] 김상배, 『버추얼 창과 그물망 방패』 (서울: 한울아카데미, 2018), 145

cybersecurity issues when it released the National Strategy for Securing Cyberspace (NSSC). According to NSSC, the cyberthreat is inevitable, and the country should coordinate to defend against its threats. It also emphasized the importance of Cold War deterrence policy to resolve cybersecurity issue.[91]

In January 2008, the Bush administration also initiated the Comprehensive National Cybersecurity Initiative (the CNCI) to make the US more secure against cyber threats.[92] The CNCI "establishes the policy, strategy, and guidelines to secure federal systems… [and]… delineates an approach that anticipates future cyber threats and technologies, and requires the federal government to integrate many of its technical and organizational capabilities to better address sophisticated threats and vulnerabilities."[93] The Obama administration initiated a comprehensive cybersecurity review and published two major reports[94] on cybersecurity policy to develop a strategic framework to ensure the CNCI is appropriately integrated, resourced, and coordinated with Congress and the private sector.[95]

Since his inauguration, Obama proposed cybersecurity as a key

[91] Richard J. Harknett and James A. Stever, "The New Policy World of Cybersecurity," *Public Administration Review* 71, no. 3 (2011): 455–60.
[92] John Rollins and Anna C. Henning, "Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations" (Congressional Research Service, March 10, 2009), https://fas.org/sgp/crs/natsec/R40427.pdf.
[93] "Fact Sheet: DHS End-of-Year Accomplishments" (Department of Homeland Security, December 18, 2008), http://www.dhs.gov/xnews/releases/pr_1229609413187.shtm.
[94] "*Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (2009)" and "*International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World* (2011)"
[95] Rollins and Henning, "Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations."

government task and presented a short- and medium-term action plan by announcing the "Cyberspace Policy Review" in 2009. According to this document, the US government defined its cybersecurity policy as:

> A policy that encompasses all the standards, policies, and strategies related to cyberspace and its internal operations and that is involved in the security and stability of the global information and communications infrastructure. It covers all aspects of threat reduction, vulnerability reduction, containment, international exchange, incident response, resilience, recovery policies and all activities, including network operations, information security, law enforcement, diplomacy, military and intelligence activities.[96]

In 2015, the Department of Defense (DoD) announced the "National Cyber Defense Strategy," a comprehensive and specific strategy for cybersecurity. The Cyber Security Strategy 2015 specifies the three duties of the Department of Defense in cyberspace: 1. Defense of the Department of Defense's networks, systems, and information; 2. Protecting the nation and national interests of the US from cyberattacks that could cause serious consequences; 3. Providing integrated cyber capabilities to support cyber military operations and emergencies, if needed.[97]

Five strategic goals are presented for this purpose. The first is to prepare personnel for the construction and maintenance of operational capability and

[96] The White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," 2009, 76.
[97] "National Cyber Defense Strategy" (Department of Defense, April 2015), https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

capacity in cyberspace, to train personnel, maintain resources. The second is to achieve effective mission through identifying, prioritizing, and defending important networks in a step-by-step manner in defense network for defense information network defense, data security and reduction of mission risk. The third is the readiness to safeguard the US and its core interests from destructive cyberattacks that could cause serious consequences. The fourth is to establish and manage the cyber operations that can control conflict intensification and lead to the formation of the conflict environment at all stages by preparing various crisis management plans. The fifth is the establishment and maintenance of strong alliances and partnerships with countries like the Middle East, Asia-Pacific and NATO for common threat prevention, international security, and stability.[98]

After taking office, President Trump announced an executive order on strengthening the cybersecurity of Federal Network and critical infrastructure in May 2017. The executive order outlined three priorities for the Trump administration in cyberspace: protecting national networks, updating antiquated and outdated systems, and directing all department and agency heads to work together.[99] The Trump administration also announced that it is planning

[98] Ibid.
[99] The White House, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," The White House, May 11, 2017, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

to write a new cybersecurity strategy because Obama-era cyber plans and strategies are fast outliving their usefulness due to the nature of technology in development.[100]

On December 18, 2017, President Trump announced the "National Security Strategy" and, like the Obama administration, recognized cyberspace as a new rising battleground and stated that the US would promise to prevent, defend and discipline malicious actors who use cyberspace capabilities to attack the US and to further improve US cyber capabilities. Trump proposed three priority actions for the US: improve attribution, accountability, and response, enhance cyber tools and expertise and improve integration and agility.[101]

The US government's cybersecurity budget has steadily increased over the past decade, reaching 16-17 percent of the IT budget since 2010 during the Obama administration compared to 8 percent during the Bush administration. Cybersecurity budget falls into IT budget, which covers organization's IT systems and services such as compensation for IT specialists, expenses related to the enterprises.[102] Of 16-17% budget, the high proportion is attributed to the cyber division budget accounting for 22 to 30 percent of the IT budgets comes from the DoD, which has the largest budget for the past five years compared to

[100] Ibid.
[101] Ibid.
[102] "What Is IT Budget (Information Technology Budget)? - Definition from WhatIs.Com," SearchCIO, accessed June 27, 2018, https://searchcio.techtarget.com/definition/IT-budget-information-technology-budget.

other federal departments. Other cybersecurity budgets in other federal government departments, except the DoD, are on the average 6-7 percent of the total IT budget for each department, similar to the 4-9 percent budget average of private companies.[103]

Meanwhile, the budget for 2017 includes $81 billion for the entire federal government's IT budget, with a cybersecurity-related budget of 22.3 percent, up from a year earlier.[104] President Trump proposed a $1.5 billion increase for the Department of Homeland Security (DHS) and a sharp increase for the DoD to protect federal networks and critical infrastructure from cyber attacks in the 2018 federal budget. Furthermore, a $ 15 billion budget for cybersecurity spending was proposed for 2019. This is another sharp increase, 4.1 percent, from the previous year.[105] As the US recognizes the importance of its cybersecurity, the government has been steadily increasing its budget to support cybersecurity strategy to secure the government infrastructure and technologies.

The Russian Strategy: The State Sovereignty

Russia began to push for a serious focus on the political implications of information security as early as the 1990s; the issue was already discussed in

[103] William L. Painter and Chris Jaikaran. "Perspectives on Federal Cybersecurity Spending." CRS Report No. R44404, February 25. 2016, ;
[104]Eric A. Fischer. "Cybersecurity Issues and Challenges: In Brief." CRS Report No. R43831, August 12, 2016.
[105] "U.S. Government: Proposed Cyber Security Spending 2019," Statista, accessed July 2, 2018, https://www.statista.com/statistics/675399/us-government-spending-cyber-security/.

1992 at the Russian Security Council.[106] The sectors of government currently responsible for information security are the Security Council, FSB, the Federal Guard Service, the Federal Technical and Export Control Service, and the Ministry of Information Technologies and Communications.[107]

In February 2016, the Special Representative of the President of the Russian Federation for International Cooperation on Information Security, Andrey Krutskikh, made a comment at the Russian national information security forum Infoforum 2016 on Russian information security. Krutskikh stated that Russia has been working on "new strategies for the information arena that would be equivalent to testing a nuclear bomb and would allow [Russia] to talk to the Americans as equals."[108] As hinted by Krutskikh's speech, Russia's strategy on information security today is characterized by its counterbalance against the US-centered order in cyberspace.

Russia's fundamental goal is to establish a global information security governance architecture that reflects Russia's national interests: complete state control in cyberspace. This is because Russian government believes that the

---

[106] Jan Softa, *Threats Against Russia's Information Society* (BookSurge Publishing, 2008).
[107] Elgin Brunner and Manuel Suter, "Russia—Critical Sectors," in *An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies*, ed. Andreas Wenger, Victor Mauer, and Myriam Dunn (Zurich: Center for Security Studies, 2008), http://www.academia.edu/1606985/International_CIIP_Handbook_2008_2009_-_An_Inventory_of_25_National_and_7_International_Critical_Information_Infrastructure_Protection_Policies.
[108] David Ignatius, "Russia's Radical New Strategy for Information Warfare," *The Washington Post*, January 18, 2017, https://www.washingtonpost.com/blogs/post-partisan/wp/2017/01/18/russias-radical-new-strategy-for-information-warfare/.

'Colour' Revolution, which led to the emergence of pro-Western regimes in Georgia and Ukraine in the mid-2000s, the Arab Spring, the democratization movement in the Middle East since 2010, and the anti-Putin protest in Russia since December 2011 were influenced by Western countries and sees such events as grave threats to national security that are just as serious as conventional security threats.[109] Moreover, Snowden's WikiLeaks pushed Russia to have more controls over the internet as US companies such as Google, Facebook, and Twitter's privacy policy pose a threat to Russia's "digital sovereignty."[110] The Russian government believes that information pertaining to Western ideologies will negatively affect Russian citizens, which would ultimately destroy the Russian social order. Therefore, the Russian government focuses on information security and tries to control the flow of the information on the Internet.[111]

In July 2013, Putin emphasized the need to address cyber threats, saying, "We need to be prepared to respond effectively to threats in cyberspace. The level of protection of related infrastructure, especially strategic installations, must be upgraded."[112] Putin has shown a high level of awareness of cyber

---

[109] 장덕준, 「[이슈브리프] 러시아의 신안보이슈」. 『국내 5 대 협력연구기관 공동기획』 (여시재, December 6, 2017), https://www.yeosijae.org/posts/356?project_id=2&topic_id=2.
[110] Nocetti, "Contest and Conquest."
[111] Keir Giles, "Internet Use and Cyber Security in Russia," *Russian Analytical Digest*, no. 134 (July 30, 2013): 12.
[112] 페트로바 아나스타시야, 「 '뒤늦은 양병(養兵)'...러시아도 올해 안에 사이버 부대 창설」. 『*Russia Beyond*』, 18 2013, https://kr.rbth.com/military_and_tech/2013/07/18/42527.

threats; cyber attacks are already being used politically and militarily, and their effects can go beyond traditional warfare.[113] Regarding cyberwarfare, terrorism, and crime-related response systems, information-related organizations are shifting their focus from the military in relation to various systems designed to respond to threats on the Internet and cyberspace.

Furthermore, Russia regards information space as a space to build the national information infrastructure and recognizes that the activities carried out within this space falls under the jurisdiction of state sovereignty. According to the "Information Security Doctrine of the Russian Federation" signed in 2016, Russia's interests in the field of information are to protect the rights of individuals to the access and use of information.[114] However, the doctrine, noting the threat to sovereignty if the information is not controlled, also included the guarantee of Russian state sovereignty over information security in the information space through the adoption of independent policies.[115] From the perspective of the Russian government's strategy of "digital sovereignty," the shift in policy from protectionist to reactionary, with the emergence of restrictive laws and regulations aimed at the Internet, occurred as a result of

[113] "Russia Must Effectively Respond to Cyber Threats, Putin Said [Rossiya Dolzhna Effektivno Reagirovat' Na Kiberugrozy, Zayavil Putin]," *RIA Novosti*, July 5, 2013, https://ria.ru/defense_safety/20130705/947885730.html.
[114] "Doctrine of Information Security of the Russian Federation [Doktrina Informatsionnoy Bezopasnosti Rossiyskoy Federatsii]" (The Ministry of Foregin Affairs of the Russian Federation, December 5, 2016), http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.
[115] Ibid

hostile rallies against Russia. The Russian cyber experts also supported the Russian government's strategy by assessing the reasons behind the Russian public's approval on the restriction of the discourse on the Web and analyzing the implications of such policies for the future.[116]

The three main characteristics of Russia's strategy on information security are as follows. First, it reflects Russia's original perception of 'cyberspace,' which is different from that of the US. Unlike the US, which emphasizes the free flow of information, Russia places considerable emphasis on regulating cyberspace as a national territory under sovereign jurisdiction.[117] Second, Russia regards competence in cyberspace as a means to enhance its national interests in the digital age. This view also illustrates Russia's perception that its cyberspace is constantly exposed to external attacks, which will inflict an enormous impact on the country. To support this approach, the Russian government has been actively establishing relevant legislative procedures such as enacting laws on cyberspace. Lastly, the governmental department in charge of cybersecurity in Russia is being switched from intelligence organizations to the military.[118] This shows Russia's intention to step up its strategy of passively analyzing given threats such as Arab Spring and anti-Putin protest to

[116] "How Does the Internet Fit into Russia's Security Strategy?," *Russia Direct*, May 4, 2016, http://www.russia-direct.org/company-news/how-does-internet-fit-russias-security-strategy?cv=1.
[117] 신범식, 「러시아의 사이버 안보의 전략과 외교」.
[118] Ibid.

aggressively expanding its cyber capabilities. It also implies that both conventional warfare and cyberwarfare can occur simultaneously.[119]

Because Russia is not advanced in the field of telecommunication technology, it is pushing for the limitation of the development in the military and public information technology in the international community to prevent the possible threat of cyberattacks as well as an arms race in information space. [120] Some countries are advancing technology that could create information warfare, and Russia fears that if it develops and uses these technologies, it could lead to attacks from foreign intelligence that could interfere in Russian domestic affairs. Therefore, Russia has been trying to incorporate traditional methods of warfare in the information space.[121]

Russian elites supported the government's policy to develop technologies and software to prevent cybercrime. Furthermore, they consider linking military forces to defensive efforts if security is not ensured at these levels. In particular, when the situation in which the state and society become unstable due to an external threat, the offensive cyber action becomes a part of Russian national security strategies.[122] This is based on the principle of non-interference

[119] 페트로바, 「 '뒤늦은 양병(養兵)'...러시아도 올해 안에 사이버 부대 창설. 」
[120] Nocetti, "Contest and Conquest."
[121] Andrew Foxall, "Putin's Cyberwar: Russia's Statecraft in the Fifth Domain." (Russian Studies Centre, May 2016), https://www.stratcomcoe.org/afoxall-putins-cyberwar-russias-statecraft-fifth-domain.
[122] Keir Giles, "Russia's Public Stance on Cyberspace Issues," in *2012 4th International Conference on Cyber Conflict (CYCON 2012)* (4th International Conference on Cyber Conflict (CYCON 2012), CCD COE, 2012), 1–13.

in domestic affairs which can be justified by their doctrine. The activities of military forces in the information space are related to the task of collecting reliable information related to threats, preventing the agitation of the possible attack, and appropriately responding to national and social threats.[123]

Furthermore, Russia increased financing of information security programs after 2010 when the US and Israel dealt a severe blow to Iran's nuclear sites during the Stuxnet Operation. The 10-20% of the national budget was allocated to the information communication system related to information security. Russia also enforced an information protection law to protect Russian national security system. Also, the Bloggers Law and the Blacklist Law, among other recent initiatives, signify growing state involvement in the Internet.[124] The Bloggers Law, which is intended to track previously anonymous bloggers, would limit the freedom of speech in cyberspace.[125] Moreover, Russian media reported in 2017 that a new law on the internet was in the process that could allow the authorities to regulate Internet traffic in the Russian server.[126]

Regarding Russia's international stance, rather than following the US-led international standard, it has been establishing an independent direction for

[123] Ibid.
[124] Neil MacFarquhar, "Russia Quietly Tightens Reins on Web With 'Bloggers Law,'" *The New York Times* (blog), December 20, 2017, https://www.nytimes.com/2014/05/07/world/europe/russia-quietly-tightens-reins-on-web-with-bloggers-law.html.
[125] Ibid
[126] Ibid.

information security and related systems.[127] The Russian government, in cooperation with members of the Commonwealth of Independent States (CIS), worked on the development of relevant legislation about cyber terrorism and computer crime. In February 1996, the 7th Session of the CIS Union Congress adopted the Basic Criminal Law, and in June 2001, a cooperative agreement against crimes in the computer information domain was concluded at Minsk, Belarus.[128] Through this, Russia, Ukraine, Belarus, Kazakhstan, and other CIS countries have integrated the relevant laws and have established a new system to cope with cyber terrorism and computer-related crimes. Thus, Russia's approach towards cyberspace can be linked primarily with restricting the creation of cyber weapon and state sovereignty and management in cyberspace.

In addition, Russia is not only working with the members of CIS, but also with international organizations such as the Collective Security Treaty Organization (CSTO), Shanghai Cooperation Organization (SCO) and BRICS (an association of five emerging national economies: Brazil, Russia, India, China and South Africa) to promote Russian norms and regulations on cyberspace in the international community.[129] Prior to the 9th BRICS summit in 2017, Putin recognized information security as an important area of BRICS' cooperation and argued that, in the short term, it needs to formulate an

[127] Giles, "Internet Use and Cyber Security in Russia."
[128] 장덕준, 「[이슈브리프] 러시아의 신안보이슈」.
[129] 신범식, 「러시아의 사이버 안보의 전략과 외교」.

appropriate international legal framework for cooperation and, in the long run, develop and adopt global rules for state action in cyberspace.[130]

2. The US and Russia's Competition in Standardization

As aforementioned, cybersecurity means various ICT systems that protect their contents from cyber attacks. However, the concept of cybersecurity is still ambiguous and not precise.[131]Currently, the US is committed to the protection of these values and principles from cybercrime through free communication and access to information, the protection of personal expression and information acquisition rights, and the promotion of individual, private, and national interests through open cyberspace by enforcing the domestic policy, international cooperation, and international norms.[132]

On the other hand, the cognitive framework for Russia's information security has been influenced by national security. In the Russian Ministry of Defense's "Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space," the Ministry first introduced norms for the Russian military's role in cyberspace. It specified the role of

---

130 "Putin Invited BRICS Countries to Conclude an Agreement on Information Security [Putin Predlozhil Stranam BRIKS Zaklyuchit' Soglasheniye Po Informatsionnoy Bezopasnosti]," *TASS*, September 1, 2017, http://tass.ru/politika/4523253.

131 Eric A Fischer, "Cybersecurity Issues and Challenges: In Brief" (Congressional Research Service, August 12, 2016).

132 신성호, 「미국의 사이버 안보 전략과 외교」. in 『사이버 안보의 국가전략: 국제정치학의 시각』, 2 (서울: 사회평론아카데미, 2017), 397.

armed forces, clarification of terms for information warfare and its legality in cyberspace. In particular, it emphasizes the national policy initiative rather than the civil society initiative because the spread of information can have a powerful influence on the public perception, which might threaten state stability.[133]

Policy

Efforts to create global standards and systems of cyberspace and cybersecurity are still at an early stage. The US is currently leading the emerging international norms of cyberspace, and in this process, the international community will soon pursue the cybersecurity-related norms, principles, and values pursued by the US. The problem is that not all nations are in agreement with the US-led international norms and governance of cyberspace.[134] In particular, Western countries, including the US and other NATO members, and non-Western countries represented by China and Russia have a different stance on international norms and principles to regulate cyber threats and attacks. Countries such as Russia and China, which oppose freedom of access to information, communication, privacy, and protection of intellectual property rights, claim that state sovereignty extends to cyberspace and states

[133] 신범식, 「러시아의 사이버 안보의 전략과 외교」

[134] McConnell et al. "Suggestions on Russia-U.S. Cooperation in Cybersecurity."; Nocetti, "Contest and Conquest."; Pasha Sharikov, "Cybersecurity in Russian-U.S. Relations," CISSM Policy Brief (Center for International Security Studies at Maryland, April 2013), http://www.cissm.umd.edu/publications/cybersecurity-russian-us-relations-0.

should be allowed to control information when necessary.[135] Russia and China also argue that the US and the West are intent on blocking the freedom of the press on the Internet to secure their own stability.[136] This eventually caused the dissatisfied challenging state to overthrow the hegemonic state's position on international order, which ultimately makes one state to compete fiercely to overcome the influence of the other state and dominate the arena. In the case of the US and Russia, Russia is fiercely challenging the US with the international order in cyberspace.

As the hegemonic state, the US promotes "open, interoperable, secure and reliable information and communications infrastructure that… strengthens international security, and foster free expression and innovation… [and] to achieve that goal, [the US] will build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships and support the rule of law in cyberspace."[137] As the US government acknowledged cyberspace as its responsibility, it criticized Russia for preferring government influence in cyberspace and limiting the free flow of information.[138] In particular, there is a major disagreement with regards to the "terrorism" issue

[135] Kulikova, "The Contest of Rules: US, China, Russia Rival in Setting the Norms of Behavior in Cyberspace."; Kawasaki, "Where Does Canada Fit in the US–China Strategic Competition across the Pacific?"
[136] Ibid.
[137] The White House, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," 2011, https://doi.org/10.1037/e688502011-001.
[138] Sergei A Medvedev, "Offense-Defense Theory Analysis of Russian Cyber Capability" (Naval Postgraduate School, 2015), http://calhoun.nps.edu/handle/10945/45225.

and "access to information space by foreign countries" that could happen in cyberspace.

According to the Russian government, "Internet sovereignty" is a guarantee that the state should have a basic influence on the information space because information can directly harm national security.[139] Russia is investing heavily in the development of software related to monitoring by the Russian government shows that Russia is making an effort to build an internet environment free from external interference.[140] In fact, the Russian government is determined to fight against the US-centric https protocol by securing the domestic "information space." In early 2016, Putin announced the RuNet 2020 plan, which is to fully deploy the Russian segment of the internet that could be disconnected from the global internet and give full sovereignty to Russia for national security purposes.[141]

In particular, when the WikiLeaks and Arab Spring broke out, many Russian political elites came to the realization that these incidents could happen to them. They saw that the Internet could become a critical threat to Russia.[142] In response, they supported measures to establish a system that could defend against external threats in a timely manner by placing restrictions on US-based

[139] Kawasaki, "Where Does Canada Fit in the US–China Strategic Competition across the Pacific?"
[140] Nocetti, "Contest and Conquest."
[141] Nocetti, "Russia's 'dictatorship-of-the-Law' Approach to Internet Policy."
[142] Giles, "Internet Use and Cyber Security in Russia."

companies such as Facebook and LinkedIn, which could spread information containing Western values to Russian citizens.[143] In July 2014, the Russian government passed laws governing the processing of personal information on information and telecommunication networks. According to the law, all companies must store personal information of Russian citizens only in databases located in the Russian Federation by September 2015, which would result in all online services falling under the Russian government's jurisdiction.[144] The law was first practiced in August 2015 against the US business-oriented social network service LinkedIn.

This law was ratified on September 1, 2015, and was first applied in August of the following year against LinkedIn. The Russian Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) blocked LinkedIn service after it failed to transfer and store Russian users' personal information in a Russian server.[145] LinkedIn had time to manage the necessary management according to Russian regulation, but it claimed that due to technical problems, the company would not be possible to transfer servers with personal information of Russians into Russian territory.[146] Moscow City Court decided to block LinkedIn in August 2016 as it violated a

[143] Ibid.
[144] "Russia" (Freedom House, October 27, 2015), https://freedomhouse.org/report/freedom-net/2015/russia.
[145] Ingrid Lunden, "LinkedIn Is Now Officially Blocked in Russia," *TechCrunch*, November 17, 2016, https://techcrunch.com/2016/11/17/linkedin-is-now-officially-blocked-in-russia/.
[146] Ibid

national law which requires all online sites to store personal information on Russian national server. In November 2016, Roskomnadzor issued an order against LinkedIn that the company was registered as a violator of the Personal Information Act, and all of its services were blocked in Russia.[147]

The US government criticized the Russian government decision to block LinkedIn. Maria Olson, the spokesman for the US Embassy in Moscow, said that the US urged Russia to resume access to LinkedIn and that Russian restrictions harmed fair competition.[148] Olson also added that "[Russian] decision is the first of its kind and sets a troubling precedent that could be used to justify shutting down any website that contains Russian user data."[149] Russian Minister of Communications and Mass Media Nikolai Nikiforov fired back, saying that "all foreign companies have to act in line with the law and there are many that have no problems respecting the legislation."[150]

A similar issue happened with a Russian company when the US government banned Kaspersky Lab. Russian IT companies have not yet played vital roles in the world market yet, but a Russian security product development company called Kaspersky Lab, with more than 500 partner companies around the world, had the opportunity to compete against the US companies in the

[147] Ibid.
[148] Christian Lowe and Maria Kiselyova, "U.S. Says Concerned over Russia Blocking Access to LinkedIn," *Reuters*, November 18, 2016, https://www.reuters.com/article/us-russia-linkedin-diplomacy/u-s-concerned-over-russia-blocking-access-to-linkedin-ria-idUSKBN13D0ST.
[149] Ibid.
[150] Ibid.

world market.[151] However, Trump's decision to exclude the product of Kaspersky Lab from the US market stopped the company from competing against other large IT companies. In June 2017, the DHS said it was concerned about ties between company officials and the Russian intelligence services, although Kaspersky Lab has repeatedly denied that it has ties to the Kremlin. However, DHS argued that Kaspersky Lab's software would be a big threat to US national security if there are any ties to the Russian government because it is widely used not only in the private sector but also in the commercial and national sector in the US.[152] So, in July 2017, Trump administration excluded Kaspersky lab from the state-of-the-art-equipment supplier list, and in September 2017, the US Senate completely forbade the use of Kaspersky Lab software because of the potential threat that the company can cause if it is related to the Russian government.[153] The Russian government condemned the Trump administration's ban on Kaspersky Lab and claimed that the US purposely carried out such a measure to eliminate any possible competition with Russia. The Press Secretary for the Russian President, Dmitry Peskov, said that "such actions run counter to fair competition… and international rules," but most importantly, "they are aimed at undermining the competitive positions

[151] "Kaspersky: Russia Responds to US Ban on Software," *BBC News*, September 14, 2017, sec. US & Canada, https://www.bbc.co.uk/news/world-us-canada-41262049.
[152] "Sands: Ban on Kaspersky Programs in the US Violates the Rules of Trade [Peskov: Zapret Na Programmy 'Kasperskogo' v SSHA Narushayet Pravila Torgovli]," *RIA Novosti*, September 14, 2017, https://ria.ru/world/20170914/1504774900.html.
[153] "Kaspersky: Russia Responds to US Ban on Software."

on the world arena of Russian companies."[154]

Internet Governance

In 1998, Russia issued a resolution entitled "Developments in the Field of Information and Telecommunications in the Context of International Security," which was adopted by the UN General Assembly. Cybersecurity began to be discussed in the United Nations disarmament and international security committee. However, the US has not responded to the resolution since its inception and has since spoken out against cybersecurity-related international cooperation. Since then, the Committee has been working with the United Nations Government Experts on Developing IT Sectors in the Context of International Security to discuss the issue of security in the international security dimension.

The role of Internet governance became very important in cyberspace. Currently, a non-profit organization called the Internet Corporation for Assigned Names and Numbers (ICANN) had been regarded as one of the most representative organizations of Internet governance. This non-profit organization coordinates IP address space allocation, root server system management, and other tasks.[155] ICANN is registered in California and is

[154]"Sands: Ban on Kaspersky Programs in the US Violates the Rules of Trade [Peskov: Zapret Na Programmy 'Kasperskogo' v SSHA Narushayet Pravila Torgovli]."
[155] "What Does ICANN Do?," ICANN, accessed June 23, 2018, https://www.icann.org/resources/pages/what-2012-02-25-en.

subject to the US Department of Commerce[156]. As a result, Russia and many other countries believe that the US has some degree of Internet governance through ICANN and further argue that US influence on ICANN is dangerous for cybersecurity as well as un-democratic and highly questionable considering recent disclosure concerning US' PRISM program.[157] Thus, Russia has recently sought to influence Internet governance by proposing Internet governance in the international arena and is attempting to challenge the US initiative in cyberspace.[158]

As mentioned earlier, the US and Russian perceptions of security differ from the terminological interpretation, so the differences also emerged between the US and Russia in its approach towards Internet governance. Because IT companies not only thrive on their own by developing technology but also accelerate the economic development of their country, telecommunications, and information, technology has become a borderless tool in current world as well as an integral part of individuals, societies, and nations. Thus, states believe that exercising influence over internet governance will bring economic benefit.[159]

However, the US and Russia take different stances on internet governance. For the US government, because there are many IT conglomerates such as

---

[156] Marika Van Laan, "ICANN, Russia, China, and Internet Reform: What You Need to Know," *Ramen IR* (blog), October 23, 2016, https://ramenir.com/2016/10/23/icann-russia-china-and-internet-reform-what-you-need-to-know/.; However, the contracted ended in 2015

[157] Ibid

[158] "Russia Moves toward Creation of an Independent Internet," *DW.COM*, January 17, 2018, https://www.dw.com/en/russia-moves-toward-creation-of-an-independent-internet/a-42172902.

[159] 김상배, 『버추얼 창과 그물망 방패』

Google and Amazon in the US, it takes a particular interest in the corporations' internal and external activities for the national benefit and asks them to participate in the internet governance to endorse US-centric norms. This can be seen as one of the reasons why the US is pushing for the freedom of the Internet in the international community and refusing to regulate the Internet. From the US perspective, state management ultimately leads to the fragmentation of the Internet, meaning the end of a free and common global Internet.[160]

Russia, on the other hand, views the free flow of information as a new kind of threat to the state after Snowden's WikiLeaks and the Arab Spring. Russia sees that the state needs to control the Internet to prevent such crisis, so it purses an internet managed by international organization or countries on the Internet governance.[161] The Institute of Information Security Issue raised two issues: "Refraining from using information and communications technology to interfere in the affairs of other states" and " Threat of use of a dominant position in cyberspace" that makes the perception inseparable from the security issue, Thus, Russia is deeply concerned about the possibility that the US will operate on an overwhelming advantage in such an information space.[162]

---

[160] Ibid., 144

[161] 김상배; Sandy Vingoe, "Cybersecurity and the Ukraine Crisis: The New Face of Conflict in the Information Age," NAOC, June 19, 2015, http://natoassociation.ca/cybersecurity-and-the-ukraine-crisis-the-new-face-of-conflict-in-the-information-age/.

[162] Sergei Modestov, "The Space of Future War [Prostranstvo Budushchey Voyny]," *Bulletin of the Academy of Military Science*, no. 2 (2003).; Keir Giles, "Russia's Public Stance on Cyberspace Issues," in *2012 4th International Conference on Cyber Conflict (CYCON 2012)* (4th International Conference on Cyber Conflict (CYCON 2012), CCD COE, 2012), 1–13.

Russia is not only focusing on strengthening the centralized cyber power. Russia is also raising its voice in the field of international cooperation to promote cybersecurity in Russia. It is true that Russia is taking a state-centered approach, but Russia was the first country to raise the need for international cooperation. Russia encouraged an international resolution that would limit the development of military and civilian information technologies that could become a threat to national security. For the Russian government, this resolution had to address the threat of cyberattacks and prevent a digital "arms race."[163] According to a recent report on Russia's critical infrastructure, the rationale for promoting such a resolution is of national interest:

> Russia's international cooperation in ensuring information security has two distinctive features: International competition for technological and information resources and for dominance in the markets has increased, and the world's leading economies have achieved a growing technological lead that allows them to build up their potential for information warfare. Russia views this development with concern, as it could lead to a new arms race in the information sphere and raises the threat of foreign intelligence services penetrating Russia through technical means, such as a global information infrastructure.[164]

There are two big focal points on the issue of establishing global cybersecurity governance. The Shanghai Cooperation Organization (SCO), led by Russia and China, and NATO, led by the US and European Union, have fundamentally different approaches towards internet governance in cyberspace.

[163] Gady and Austin, "Russia, The United States, And Cyber Diplomacy: Opening the Doors."
[164] Ibid, 6 from A. A. Streltsov, "State Information Policy: The Basis of the Theory [Gosudarstvennaya informatsionnaya politika: osnovy teorii]"

While Russia favors creating borders in cyberspace, the US is opposed to the establishment of "cyberspace borders."[165] The US government sees it as a direct challenge to democratic principles and a justification by governments on limiting the free flow of information. In a number of statements on cybersecurity, particularly in Article 19 of the Universal Declaration of the Human Rights, US officials have outlined and emphasized the freedom of individuals to seek, receive, and communicate information and ideas.[166]

The West emphasizes that freedom of expression, openness, and trust should be established as basic principles in the Internet and cyberspace. It is also essential to establish an international norm that harmonizes all the opinions of various members such as individuals, industries, civil society, and government agencies that use cyberspace.[167] It emphasizes the importance of establishing and implementing Confidence Building Measures (CBMs) applicable to cyberspace to reduce threats and increase trust in cyberspace rather than establish new norms in the West. The primary position of the West is that it contains the intention of checking the use of the Internet as a tool of governance in the domestic politics by limiting and controlling the freedom of

[165] Ibid.
[166] The White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure."
[167] Ciolan, "Defining Cybersecurity as the Security Issue of the Twenty First Century. A Constructivist Approach."; 김상배. 「네트워크로 보는 세계정치의 변화: 사이버 안보와 디지털 공공외교를 중심으로」. April 2012. 제주평화연구원.

the press, such as China and Russia.[168]

On the other hand, in the anti-Western side led by Russia and China, they argue that state sovereignty should be recognized in cyberspace, and if necessary, should remain as a domain where information control is possible. Therefore, it is impossible to accept the dominance of Western unilateralism on the Internet and cyberspace, and it is necessary to establish a fairer world order in cyberspace. They are more urgent to agree on the rules for international information security actions based on the nation's Internet control.[169] Today, Russia is at the forefront of advocating for the internationalization of Internet governance under the United Nations and the guarantee of digital equality and sovereignty of all nations, together with BRICS and Shanghai Cooperation Organization (SCO) partners. In particular, in order to have digital sovereignty, the Russian government believes that each country should have its search engine so that the country's information is not taken over by Western corporations like Google.

The difference between the US and Russia's views is best shown by the opinions each has expressed about the role of the International Telecommunication Union (ITU). The ITU is a specialized agency of the United Nations and an international intergovernmental organization aimed at promoting international cooperation for the improvement and efficient use of

[168] Nocetti, "Russia's 'dictatorship-of-the-Law' Approach to Internet Policy."
[169] 장덕준, 「[이슈브리프] 러시아의 신안보이슈」.

telecommunications.[170] In December 2012, Russia and other countries submitted proposals to the World Conference on International Telecommunication (WCIT-12) with the aim to redefine the internet as a government-controlling system.[171] Furthermore, these proposals would give the ITU the authority to exercise jurisdiction over the Internet governance function entrusted to international NGOs.[172]

However, the US opposed the signing of the treaty, as it saw the treaty as an attempt by Russia, Iran, and other nations to expand government control over the Internet.[173] Nevertheless, this proposal was signed in December 2012 by 89 nations, including Russia, despite the US and 54 other nations' objections.[174] In short, since there is no consensus on the authorities of the ITU, the US and its allies decided to follow one international telecommunications standard, while Russia and the rest of the world decided to stick to another standard.

Another issue that illustrates the different approaches of the US and Russia to Internet governance is the Convention on Cybercrime. The Convention on

[170] "ITU: Committed to Connecting the World," ITU, accessed July 23, 2018, https://www.itu.int/en/Pages/default.aspx.
[171] Violet Blue, "WCIT-12 Leak Shows Russia, China, Others Seek to Define 'Government-Controlled Internet,'" *ZDNet*, December 8, 2012, https://www.zdnet.com/article/wcit-12-leak-shows-russia-china-others-seek-to-define-government-controlled-internet/.
[172] Ibid
[173] Alex Fitzpatrick, "U.S. Refuses to Sign UN Internet Treaty," *CNN*, December 14, 2012, https://edition.cnn.com/2012/12/14/tech/web/un-internet-treaty/index.html.
[174] Danielle Kehl and Tim Maurer, "Did the U.N. Internet Governance Summit Actually Accomplish Anything?," *Slate*, December 14, 2012, http://www.slate.com/blogs/future_tense/2012/12/14/wcit_2012_has_ended_did_the_u_n_internet_governance_summit_accomplish_anything.html.

Cybercrime, also known as the 2001 Budapest Convention, is the first international treaty that sought to address internet and computer crime by unifying national laws.[175] The US signed this treaty along with 55 nations because it is in a position to cooperate in the fight against the use of internet technology for criminal purposes.

However, Russia opposed the convention, stating that its adoption would violate Russian state sovereignty by allowing other countries to have unauthorized access to the IT environment, and illegally use IT resources, computer systems, and information through agreements.[176] In fact, Russia is preparing a new convention because the current document does not do justice to Russian sovereignty[177] According to *Moscow Daily,* the Russian government had proposed a new "United Nations Convention on Cooperation in Combating Information Crimes" that is "innovative" and "universal" to replace the 2001 Budapest Convention.[178] However, US cyber experts worried that if the new convention is drafted, it will enhance Russia's ability to control communication within its own borders and gain access to communications in other states.[179]

. Cyberspace is associated with international disputes, and the Internet is

[175]"Convention on Cybercrime," European Treaty Series (Budapest: Council of Europe, 2001), https://www.coe.int/en/web/conventions/full-list.
[176]John Markoff and Andrew E. Kramer, "U.S. and Russia Differ on a Treaty for Cyberspace," *The New York Times*, June 27, 2009, sec. World, https://www.nytimes.com/2009/06/28/world/28cyber.html.
[177] "Russia Calls for Internet Revolution," *RT World News*, 2012, https://www.rt.com/news/itu-internet-revolution-russia-386/.
[178] Ignatius, "Russia's Radical New Strategy for Information Warfare."
[179] Ibid

becoming increasingly internationalized. In 2020, more than 90% of Internet users are expected to reside in non-Western countries, especially non-OECD countries, which Russia seems to be aware of and explains the strong questioning of US leadership in Internet space. Thus, Russia insists on the internationalization of Internet management by emphasizing the nature of the Internet as a "global public good."[180] The difference between the basic positions of the US and Russia and the competition this forms has created a global faultline around cyberspace, and the task to overcome is to establish global governance related to cybersecurity.[181]

3. The US and Russia's Militarization in Cyberspace

The biggest reason why nuclear deterrence worked between the US and USSR during the Cold War was MAD, which is a doctrine of military strategy and national security policy. [182] The US has been the most prominent leader and beneficiary of cyberspace, but it has also been the most prominent target of cyberattack. FireEye Chief Executive Officer Kevin Mandia said countries with more advanced technology would be more vulnerable to cyberattacks. Therefore, Russia would win if cyber war happens between the US and Russia because even though the US has advanced technology, it relies on the internet

[180] Jovan Kurbalija, *An Introduction to Internet Governance* (Msida, Malta: Diplo Foundation, 2010).
[181] 신범식, 「러시아의 사이버 안보의 전략과 외교」
[182] Trujillo, "The Limits of Cyberspace Deterrence."

and other online infrastructure more than Russia.[183]

Kremlin's senior advisor Krutskikh also warned that the cyber competition between the US and Russia has already begun and that the cyber cooperation between US and Russia became in question and entered the preparedness for cyberwarfare as the US-Russia relationship has worsened since the Ukrainian crisis[184].

US CYBERCOM

The 2015 US National Security Strategy made it clear that the world is already in the midst of a cyber war involving hackings and espionage aimed at national infrastructure. In fact, according to Principal Deputy Under Secretary Defense for Policy James Miller in 2011, the US had more than 1.8 billion cyber attacks just on the IT system of Congress and other agencies each month. Deputy Secretary of Defense William J. Lynn, III, said that there are more than 100 foreign intelligence agencies who have tried to breach DoD computer networks.[185] The security and economy of the advanced countries have already developed in a way that is deeply integrated to IT infrastructure; and to the countries that oppose the direction of global economic development; and to the

[183] Ell, "FireEye CEO."
[184] Julianne Smith and Adam Twardowski, "The Future of U.S.-Russia Relations," Strategy & Statecraft (Center for New American Security, January 2017), https://www.cnas.org/publications/reports/the-future-of-u-s-russia-relations.
[185] Principal Deputy Under Secretary of Defense for Policy James Miller in testimony before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities on February 10, 2011.; William J. Lynn, III's Remarks on Cyber at the RSA Conference on February 15, 2011.

use of these infrastructures to achieve the malicious cybercrimes are emerging as a significant threat to this infrastructure. The problematic countries that the US says are Russia, Iran, North Korea and China, and Western experts all agreed that the US sees Russia as a major threat. In May 2015, *Newsweek* published an article entitled "Russia's Greatest Weapon May Be Its Hacker," which states that the US has identified Russi as the most powerful challenger of the ongoing cyber war.[186] The article further stated that Russian cyber capabilities are underestimated, and hackers in Russia are referred to as the most creative and outstanding cyber warriors in the field.[187]

Even though the US values "free flow of information," due to increasing fear of national security threatened in cyberspace, it is militarizing in the cyber domain for defensive reasons.[188] As scholars have warned, the US has been the biggest target of cyberattacks.[189] In January 2016, James Clapper, the former Director of National Intelligence, categorized cyber threats as a high security threat to the US from 2013 onward, and that in the post-9/11 world, "'cyber' bumped 'terrorism' out of the top spot on [US] list of national threats" during a

[186] Owen Matthews, "Russia's Greatest Weapon May Be Its Hackers," *Newsweek*, May 7, 2015, https://www.newsweek.com/2015/05/15/russias-greatest-weapon-may-be-its-hackers-328864.html.
[187] Ibid.
[188] "Competition in Cyberspace," *Armed Forces Journal*, January 1, 2013, http://armedforcesjournal.com/competition-in-cyberspace/.
[189] Ell, "FireEye CEO."

speech for the Naval Academy's Cyber Lecture Series.[190]

The US recognizes cyberspace as a new battleground and uses its own Cyber Command instead of the cyber countermeasures organization, which was maintained as a loose joint task force until 2009. In June 2009, the US established the US Cyber Command (USCYBERCOM) as part of the US Strategic Command (STRATCOM). This Command was created for defensive purposes, unifying different governmental sectors' cyberspace operations and strengthening the DoD's cyberspace capabilities. When the Cyber Command was newly established under STRATCOM, a four-star general was assigned as the Commander to reflect its importance.[191] Furthermore, the creation of USCYBERCOM re-emphasized cyberspace as a battlefield. Thus, the DoD must be ready to conduct and carry out operations.

USCYBERCOM operates and defends their portion of the DoD Information Networks (DODIN); performs full-spectrum cyber operations, meaning offensive and defensive; provides cyber training and education, and undertakes cyber research and capabilities development for their respective services.[192] USCYBERCOM also oversees US space operations, global strike,

[190] Aaron Boyd, "DNI Clapper: Cyber Bigger Threat than Terrorism," *Federal Times*, February 4, 2016, https://www.federaltimes.com/management/2016/02/04/dni-clapper-cyber-bigger-threat-than-terrorism/.
[191] William Jackson and 2009 Jun 24, "DOD Creates Cyber Command as U.S. Strategic Command Subunit," *FCW*, accessed July 23, 2018, https://fcw.com/articles/2009/06/24/dod-launches-cyber-command.aspx.
[192] Andrew Feickert, "The Unified Command Plan and Combatant Commands: Background and Issues for Congress," n.d.

and global missile defense. In recent years, with growing fears of cyberattack and terrorism, the US government increased the Cyber Division budget from $346.5 million in 2009 to $810 million in 2014.[193] In 2015, USCYBERCOM expanded and added 133 teams, and then, in 2016, these new teams had achieved "initial operating capability" (IOC). Though, IOC is not the same as combat readiness, it was the first step in that direction.[194]

On August 18, 2017, President Trump announced that USCYBERCOM is to be elevated to the status of a full and independent Unified Combatant Command (CCMD), putting it on the same level as other combatant commands that operate in the Middle East, Europe and elsewhere to resolve against cyberspace threats in more offensive approach.[195] This means that the head of USCYBERCOM will eventually report directly to the Secretary of Defense.[196] USCYBERCOM's agenda is to plan, coordinate, integrate and conduct activities to direct the operations and defense of specified units and networks. It also prepares to conduct cyber-military operations to enable actions in all domains, ensure the US and allies' freedom of action in cyberspace and deny the same to the opponent, and defend opponent's attempts to interfere with

[193] Craig and Valeriano, "Conceptualising Cyber Arms Races."
[194] Boyd, "DNI Clapper: Cyber Bigger Threat than Terrorism."
[195] The White House, "Statement by President Donald J. Trump on the Elevation of Cyber Command," The White House, August 18, 2017, https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/.
[196] Ibid.; Crowther, "National Defense and the Cyber Domain."

CCMD operations.[197]

Because the US promotes freedom in cyberspace and the concept of cyber threats was vague, there had been concerns on whether the military has right to respond to cyber attacks, General Keith B. Alexander stated that the "command is not about an effort to militarize cyberspace… Rather, it's about safeguarding [US] military assets" from the enemy. General Alexander further noted that the USCYBERCOM would follow a legal framework and that the purpose of the command is not overshadowed any civilian activities in cyberspace.[198]

Russia's Information Warrior

Russia's agenda on information security is complete militarization in cyberspace, which is the reason why the Russian government put significant resources into information security for the strategic purpose. Because Russia realizes that its cyber capabilities are behind the US cyber capabilities, it has been trying to incorporate traditional methods of warfare in the information space.[199] In fact, Russia is currently the only country that has combined cyberwarfare with traditional warfare. Russia views cyber capabilities as tools of information warfare, which it combines "intelligence, counterintelligence,

[197] "U.S. Strategic Command: Factsheets," U.S. Strategic Command, accessed June 23, 2018, http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/.
[198] Ell, "FireEye CEO."; Jeff Daniels, "US Could Potentially Lose next War to Russia or China, Warns Rand," *CNBC*, 2017, https://www.cnbc.com/2017/12/09/us-could-potentially-lose-next-war-to-russia-or-china-warns-rand.html.
[199] Foxall, "Putin's Cyberwar: Russia's Statecraft in the Fifth Domain."

maskirovka, disinformation, electronic warfare, debilitation of communications, degradation of navigation support, psychological pressure, and destruction of enemy computer capabilities."[200]

For example, during the war against Georgia in 2008, Russian ground attacks were accompanied by a widespread cyber attack on government websites, marking the first kind of hybrid war. Russian hackers launched a series of Distributed-Denial-of-Service (DDoS) attacks, blocking crucial sections of Georgian internet traffic as well as striking Georgian government sites with Russian propaganda.[201] Furthermore, since 2014, Russia's hybrid war, especially with Ukraine, has included cyberattacks on energy infrastructure as well as government and media websites.[202] It is a well-known fact that Russian-backed separatist forces sabotaged the networks of the Ukrainian phone company, UKrtelecom, by disabling the phones of government officials in Kiev. Russian troops also deployed GPS and radar jammers to isolate the region.[203] Many cybersecurity analysts suspect that the Russian government has infiltrated the Ukrainian government's system using a virus called "Snake" since 2010.[204]

Russian newspaper *RIA Novosti* reported that the Ministry of Defense was

[200] Giles, "'Information Troops' - A Russian Cyber Command?"
[201] Vingoe, "Cybersecurity and the Ukraine Crisis."
[202] Foxall, "Putin's Cyberwar: Russia's Statecraft in the Fifth Domain."
[203] Vingoe, "Cybersecurity and the Ukraine Crisis."
[204] Ibid

planning to create a special unit dedicated to information security in 2013.[205] This unit monitors information coming from outside the country and carries out the task of blocking the cyber threats so that it will have similar functions to cyber units created by the US. The creation of a cyber unit seems to have been pursued in 2012 and 2013 after Deputy Prime Minister Dmitry Rogozin and Minister of Defense Sergey Shoygu proposed preparing the cyber command for armed troops (Information soldiers) under the General Staff.[206]

In May 2014, Russia decided to create an interdepartmental unit for the security of military command communication systems. The Russian command and control system will be digitized and will build an integrated system of reconnaissance means, target designation, and control of the army and weapons. Also, in addition to the existing combat troops, a unit of the Russian army is also known as the "Scientific Forces (научный эскадрилья)," which are dedicated to cope with operations to access information of enemy countries and influence their decision-making structure. The personnel of this unit includes not only the professional personnel in universities and the private sector but also cyber professionals that are employed among criminals related to hacking and computers.[207] According to the Russian newspaper *Kommersant*, Russia now has cyber hacker units with around 1,000 hackers, and these units operate

[205] "Russia Must Effectively Respond to Cyber Threats, Putin Said [Rossiya Dolzhna Effektivno Reagirovat' Na Kiberugrozy, Zayavil Putin]."
[206] 페트로바, 「 '뒤늦은 양병(養兵)'...러시아도 올해 안에 사이버 부대 창설. 」
[207] 장덕준, 「[이슈브리프] 러시아의 신안보이슈」.

with a massive £250 million budget.[208] This led Russia to be able to operate cyber units and related organizations in earnest, to respond to cyber threats defined by Russia, and to have an effective military organization to intervene to secure national interests actively.

In 2015, the structure of "Science Force" was further developed. The Science Force had further development in the structure. According to *Moskovskij Komsomolets*, the new structure would have programmers, mathematicians, cryptographers, electronic warfare officers and communications experts who would collaborate to prevent cyber attacks from the Internet and other military networks such as the missile defense system's network.[209] The Russian government's claim that these forces are for the defensive purposes because Russia is far more vulnerable in cyberspace than its opponent, the US.[210] However, security analyst Keir Giles argued that Russia's intention to form a cyber unit is to create an "all-encompassing cyber military force" to engage in attacks on enemy territory.[211] Western experts already agreed that the ability of Russian hackers is at the top of the world and that Russia is "conducting offensive cyberactivites."[212] They further argued that

[208] Maria Kolomychenko, "On the Internet, Cyberwars Have Been Introduced [V Internet Vveli Kibervoyska]," *Kommersant*, October 1, 2017, https://www.kommersant.ru/doc/3187320.
[209] Robert Beckhusen, "The Russian Military Creates Its Own Cyber Troops," *War Is Boring* (blog), May 28, 2015, https://warisboring.com/the-russian-military-creates-its-own-cyber-troops/.
[210] Ibid
[211] Giles, "'Information Troops' - A Russian Cyber Command?"
[212] Matthews, "Russia's Greatest Weapon May Be Its Hackers."

FSB infected to spy on foreign tourists' technologies such as laptops and cell phones by deploying aggressive cyberspy tools.[213]

4. Russiagate: The Beginning of the US-Russia Cyber War?

Cyberattacks have become a common phenomenon ever since the DDoS attack against Estonia in 2007. New viruses are created each year, causing considerable damage to governments and companies. Countries like the US, the United Kingdom, Russia, and China have tried to work together to create harmonized laws and unified consensus on cyberspace. It ultimately failed due to the different perceptions they have of cyberspace.[214] However, Russian interference in the US 2016 election changed the perception of the importance of the threat of cyberattacks decisively and appeared to mark the start of a new kind of competition between the US and Russia.

Russian Interference in the US 2016 Election

In June 2016, DCLeaks and Guccifer 2.0[215] published a collection of Democratic National Committee (DNC) emails.[216] The collection included

[213] Ibid.
[214] Cerrudo, "Why Cybersecurity Should Be The Biggest Concern Of 2017."
[215] DCLeaks is a website that published Clinton's emails and Guccifer 2.0 is a hacker who claimed to hacked into DNC. Both are specifically mentioned as fronts for Russian GRUs in Mueller's indictment.
[216] Raphael Satter, Jeff Donn, and Chad Day, "Inside Story: How Russians Hacked the Democrats' Emails," *US News & World Report*, November 6, 2017, https://www.usnews.com/news/world/articles/2017-11-03/inside-story-how-russians-hacked-the-democrats-emails.

emails from the personal accounts of seven key DNC staff members who worked for Hilary Clinton's campaign.[217] This leaked data adversely affected Clinton's public image in the election. The Democratic Party claimed that Russian intelligence agencies and officials had hacked the server. Clinton further pushed for the accusation, stating that people all "know that Russian intelligence services, which are part of the Russian government, which is under the firm control of Vladimir Putin, hacked into the DNC…and [Trump] praise for Putin… is… quite remarkable" during the 'Fox News Sunday.'[218] Russia denied all accusations. Russian Foreign Minister Sergei Lavrov said in an interview with *CNN* that the blame for Russia is not backed by facts.[219] Putin also insisted that the DNC server hack was not in line with Russia's interests and that the Russian government had nothing to do with it.[220]

Obama ordered US intelligence agencies to investigate the case. The Office of the Director of National Intelligence (ODNI) and the Department of Homeland Security (DHS) concluded that the Russian government was involved in the hacks. According to a joint statement by the ODNI and the DHS, the Russian government directed hacks to leak personal data from the DNC server and the Clinton campaign's email accounts. The assessment was made

---

[217] Ibid
[218] Ibid
[219]"Foreign Minister Sergey Lavrov's Interview with Amanpour Program on CNN International, Moscow, 12. October 2016."
[220] "International Forum 'Arctic - Territory of Dialogue' [Mezhdunarodnyy Forum «Arktika – Territoriya Dialoga»]" (Kremlin), accessed June 23, 2018, http://kremlin.ru/events/president/news/54149.

by ODNI that the Russian government interfered in the US presidential election because President Putin favored presidential candidate Trump over Clinton.[221] Russia still denied all accusations regarding its involvement in US election-related hacks or leaks.[222]

In January 2017, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) coordinated and drafted an analytic assessment on the motivation and scope of Russia's intentions regarding the US election. These three agencies also concluded that Putin interfered in the US election because he preferred Trump's policy toward Russia. It was also revealed that the Russian government had used a multifaceted propaganda operation that covered US primary campaigns, think tanks, social media such as Facebook and Twitter and even news outlets to influence the election.[223]

On July 14, 2018, the Department of Justice (DOJ) indicted against 12 Russian intelligence agents as part of special counsel Robert Mueller's investigation of Russian interference in the 2016 election. The department accused them of engaging in a 'sustained effort' to hack Democrats emails and

[221] Joint statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security (DHS).
[222] Rid, "All Signs Point to Russia Being Behind the DNC Hack."
[223] "Assessing Russian Activities and Intentions in Recent US Elections" (Intelligence Community Assessment, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.

computer networks.[224] According to Mueller, these 12 Russian agents were under the Main Intelligence Directorate of the General Staff (GRU).[225]

However, Russia continues to deny all allegations on the Russian interference of the 2016 election. Putin had an interview with *Fox News* after a presidential summit in Helsinki with Trump on July 16, 2018. He stated that Russia had never meddled in the US election and that the allegation is "utterly ridiculous."[226] On the same day, Trump also spoke to *Fox News*, stating that he has "great confidence in [the US intelligence], but… Putin was extremely strong and powerful in his denial."[227] At a press conference, Trump called Mueller's investigation "ridiculous" and a "total witch hunt" that is preventing improved relations between the US and Russia.[228] Trump's statement has been heavily criticized by both Houses of Congress and the Intelligence Community as nothing but "treasonous." Daniel Coats, the Director of National Intelligence, reaffirmed the Intelligence Community's assessment of "ongoing, pervasive

[224] Katelyn Polantz and Stephen Collinson, "Mueller Probe: 12 Russians Indicted for DNC Hack," *CNN*, July 14, 2018, https://edition.cnn.com/2018/07/13/politics/russia-investigation-indictments/index.html.
[225] Abbreviated from Russian name "*Glavnoye razvedyvatel'noye upravleniye"*
[226] Phillip Rucker, Anton Troianovski, and Kim Seung Min, "Trump Hands Putin a Diplomatic Triumph by Casting Doubt on U.S. Intelligence Agencies," Washington Post, July 16, 2018, https://www.washingtonpost.com/politics/ahead-of-putin-summit-trump-faults-us-stupidity-for-poor-relations-with-russia/2018/07/16/297f671c-88c0-11e8-a345-a1bf7847b375_story.html..
[227] Ibid.
[228] Julie Davis, "Trump, at Putin's Side, Questions U.S. Intelligence on 2016 Election," *The New York Times*, July 16, 2018, https://www.nytimes.com/2018/07/16/world/europe/trump-putin-election-intelligence.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=a-lede-package-region&region=top-news&WT.nav=top-news.

efforts to undermine [US] democracy."[229] Senator John McCain called Trump's action as "one of the most disgraceful performances by an American president in memory."[230]

Aftermath

This affair has posed a serious threat not just to the Democrats, but also to the national security of the US. According to a DHS statement released on January 6, 2017, national infrastructure related to elections is now seen as a critical infrastructure for national security.[231] This means that infrastructure associated with elections must meet federal standards of cybersecurity. Thus, the US began to see Russia's cyber attacks not as ordinary cyber crimes but as infringements of national security.[232]

The speculation of Russia's intervention in the US presidential election has produced another important result. It made the US reserve the direction of the cybersecurity discourse. In December 2008, before Obama took office, the Center for Strategic and International Studies (CSIS) published a report on the recommendation of "Securing Cyberspace for the 44th Presidency." This report stated that "a major goal of the US should be to promote international

[229] Rucker et al. "Trump Hands Putin a Diplomatic Triumph by Casting Doubt on U.S. Intelligence Agencies.""
[230] Ibid.
[231] "Statement by Secretary Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector | Homeland Security," Homeland Security, 2017, https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.
[232] Polantz and Collinson, "Mueller Probe: 12 Russians Indicted for DNC Hack."

cooperation for infrastructure management."[233] In 2016, CSIS published a new report just before Trump's inauguration. It states that the US faces a major challenge in strengthening international cooperation with its allies against cyber-aggressors. The report also argued that "the key to a [US] cybersecurity strategy ... lies with changing the behavior of hostile states. This requires norms for responsible state and company behavior, building cybercrime cooperation, and shaping opponent behavior through interaction and consequences."[234] Unlike the 2008 report, when the word "Russia" was never mentioned, the 2016 report referred to Russia 8 times as a threat to cyberspace. Russia, along with China and Iran, was also referred to as the US' principal cyber opponents[235].

Concern about Russian influence on cyberspace began to be raised in different parts of the US government. In December 2016, the US imposed sanctions against Russia and expelled 35 Russian diplomats when it officially accused Russia of intervening in the US presidential election in 2016.[236] In early 2017, the two committees of the US Senate, the Military Commission, and the Intelligence Committee, held hearings on external cyber threats, in particular on Russian behavior.[237] In addition, the US Congress proposed more

[233] James R. Langevin et al., "Securing Cyberspace for the 44th Presidency:" (Fort Belvoir, VA: Defense Technical Information Center, December 1, 2008), https://doi.org/10.21236/ADA489361.
[234] Whitehouse, "From Awareness to Action: A Cybersecurity Agenda for the 45th President."
[235] Ibid.
[236] Sheldon Whitehouse, "From Awareness to Action: A Cybersecurity Agenda for the 45th President," January 2017, 34.
[237] "Foreign Cyber Threats to the United States," § Senate (2017), https://www.armed-services.senate.gov/hearings/17-01-05-foreign-cyber-threats-to-the-united-states.

than 40 legislative measures in the first half of 2017, including blaming Russia. In June 2018, the US Department of Treasury imposed new sanctions on five Russian entities and three individuals in the connection to Russian interference during the 2016 election.[238] However, further US action towards Russia is in question since Trump denied the allegation, disregarded the indictment, supported Russia, and blamed the Obama administration for the attack if it really happened.[239]

5. Analysis of the US and Russia's Cyber Competition

Krutskikh, a Special Representative of President Putin, told his audience at Infoforum 2016 in Moscow:

> You think we are living in 2016. No, we are living in 1948. And do you know why? Because in 1949, the Soviet Union had its first atomic bomb test. And if until that moment, the Soviet Union was trying to reach agreement with [President Harry] Truman to ban nuclear weapons, and the Americans were not taking us seriously, in 1949 everything changed and they started talking to us on an equal footing…. I'm warning you: We are at the verge of having 'something' in the information arena, which will allow us to talk to the Americans as equals.[240]

Krutskikh stressed the importance for Russia of having a strong hand in this new domain of cyberspace. If Russia is weak, he explained, "[Russia] must

[238] Donna Borak and Nicole Gaouette, "US Unveils New Russia Sanctions over Cyberattacks," *CNN*, June 11, 2018, https://www.cnn.com/2018/06/11/politics/us-russia-cyber-sanctions/index.html.
[239] Polantz and Collinson, "Mueller Probe: 12 Russians Indicted for DNC Hack."
[240] Ignatius, "Russia's Radical New Strategy for Information Warfare."

behave hypocritically and search for compromises. But once [Russia] becomes strong, [she] will dictate to the Western partners [the US and its allies] from the position of power."[241]

There have been several attempts between the US and Russia to cooperate on cyber issues, as the two states recognize the importance of shared international norms and regulations. The primary interest of both the US and Russia in cyberspace is the protection and control of national defense assets and cyber intelligence and information.[242] Incidents such as Snowden's WikiLeaks, Russia's Ukrainian intervention, and 2016 US election interference have exacerbated bilateral relations. However, the failure of cooperation is primarily due to the fundamental difference between the two states in their perception of cyberspace.

The most fundamental conflict between Russia and the US comes from the US government's emphasis on the free flow of information, whereas the Russian government prioritizes public security and state control of information. The Russian government believes that 'free flow of information' needs to be constrained by legislation and the need for anti-terrorism.[243] In particular, Russia's position on terrorism and cyber terrorism made it difficult for the two

[241] Ibid
[242] Brad Karp, "Federal Guidance on the Cybersecurity Information Sharing Act of 2015," *Harvard Law School Forum on Corporate Governance and Financial Regulation* (blog), March 3, 2016, https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/.
[243] Giles, "'Information Troops' - A Russian Cyber Command?" from I. Shchegolev, in *London Conference on Cyberspace*, 2011.

sides to agree on common measures.[244] There is the 'risk perception' that Russia is feeling at the base of the different views between the US and Russia, which makes it difficult for Russia to fully accept the US position on cyber norms.[245] Russia believes that information is a national asset that needs to be controlled by the state to ensure its national security. The risk of critical information being leaked to other countries is a grave threat that could harm the country. To prevent such leakages internally, Russia implemented laws that would make anonymous posting illegal, and all corporate data has to be stored in Russian servers.[246] In order to protect the information from external threats, Russia has been aggressively working toward the creation of international agreement in cyberspace. Russia submitted a proposal to WCIT-12 to give ITU legal authority on the Internet governance. It also drafted a new convention to replace the 2001 Budapest Convention that would give Russia to exercise its authority in its own networks.[247]

However, the US government is skeptical of the Russian government's position on the establishment of the international agreement because it could provide cover for Russia's legitimacy on censoring the Internet and limiting

[244] Anna-Maria Talihärm, "CyberTerrorism: In Theory or in Practice?," *Defence Against Terrorism Review* 3, no. 2 (2010): 59–74.; Andrew Monaghan, "The Moscow Metro Bombings and Terrorism in Russia," no. 59 (2010): 12.
[245] "Public Law 114-113, Division N, Title IV, Section 402" (DEPARTMENT OF STATE INTERNATIONAL CYBERSPACE POLICY STRATEGY, 2016), https://www.state.gov/documents/organization/255732.pdf.
[246] MacFarquhar, "Russia Quietly Tightens Reins on Web With 'Bloggers Law.'"
[247] Blue, "WCIT-12 Leak Shows Russia, China, Others Seek to Define 'Government-Controlled Internet.'"

public access to information.[248] Due to its emphasis on democratic values, the US government believes that controlling and censoring cyberspace is anti-democratic. From the beginning, the US has been calling for 'free flow of information; that anyone has his or her right to freely access any information, express and communicate with others. According to the former Secretary of State Hilary Clinton, all countries should promote the free flow of information, which also has the positive effect of promoting democracy. Cyberattacks and cyber threats should be prevented through cooperation among states and not by controlling cyberspace. [249] This gap between the US and Russia in their approach towards cyberspace makes it difficult for the two states to cooperate in cyberspace.

The pivotal moment of the US and Russia's competition in cyberspace was when Russia alleged with interfering in the 2016 US election. It changed the US stance on Russia and cybersecurity. It is true that this was not the first time that Russia has interfered in another country's election. In fact, there have been 27 Russian electoral interventions in foreign countries since 1991. Besides, the US also has interfered in other countries' elections. For example, the US has interfered with the Serbian election in 2000 to tilt the election in favor of candidates with more pro-American values.[250] According to ICA in the 2016

[248] Gady and Austin, "Russia, The United States, And Cyber Diplomacy: Opening the Doors."
[249] "Hillary Clinton's Historic Speech on Global Internet Freedom."
[250] Alex Ward, "'It's Probably Going to Get Worse': A Former Top Intel Official on Russia Election Meddling," Vox, February 27, 2018,

election, Putin considered Trump to have a Russia-friendly position on Syria and Ukraine and preferred his policy positions.

However, Russian interference in the 2016 US election is critical because if the allegations are true, it is an attack that threatens US national security.[251] Note that this was not a militaristic cyberattack that Russia has been doing to other countries, like Estonia and Ukraine.[252] Russia did not incorporate conventional capabilities with its cyber capabilities; it solely used its cyber capability to infiltrate the DNS server and further into the voting systems.[253] If the allegation is true, this undermined and threatened the democratic value that the US holds greatly.[254] Some wonder why the US did not immediately respond to Russia's interference. Two main reasons were because the current president refuses to blame Russia publicly and the event occurred in cyberspace. Because cyberspace allows people to be anonymous, it is difficult to quickly identify the attacker. Different intelligence agencies in the US conducted assessment and confirmed that the Russian government had instructed hackers to infiltrate the US election, and special counsel Mueller has indicted 12 GRU members.[255]

https://www.vox.com/world/2018/2/27/17046300/russia-election-meddling-hack-treverton-interview.

[251] Stephen F. Cohen, "'Russiagate' Zealots (Mainly Democrats) Have Become a Major Threat to US National Security," *The Nation*, November 15, 2017, https://www.thenation.com/article/russiagate-zealots-mainly-democrats-have-become-a-major-threat-to-us-national-security/.

[252] "Assessing Russian Activities and Intentions in Recent US Elections."

[253] Ibid

[254] "Hillary Clinton's Historic Speech on Global Internet Freedom"

[255] Polantz and Collinson, "Mueller Probe: 12 Russians Indicted for DNC Hack."; Joint statement from the Department of Homeland Security and Office of the Director of National

However, even though there are numerous reports and stories that point to Russia, most of them are merely speculations. There is no concrete evidence of the allegation that proves Russia was behind it, and Russia and Trump vehemently refuse the allegations.[256]

Regardless of the allegation, the US is currently concerned that that creating an international agreement and regulation in cyberspace would be ineffective because it would be impossible to find if a cyber attack was initiated by a foreign government, government-backed hackers or an independent contractor.[257] Russian interference in the election clearly demonstrated this fear. Deterrence does not work in cyberspace as the high level of cross-border connectivity and anonymity makes it easier for an aggressor to attack and hide and harder for defenders detect and trace.[258] Mostly, the plausible evidence is hard to find, and even if they have evidence, it takes too much time to respond. Even with the indictment of the 12 Russian agents in relation to the 2016 US election, some—including President Trump—continue to deny the allegations, arguing that there is no physical evidence tying the allegations back to Russia.[259]

Intelligence on Election Security.; "Assessing Russian Activities and Intentions in Recent US Elections."

[256] Aaron Mate, "Russiagate Is More Fiction Than Fact," *The Nation*, 2017, https://www.thenation.com/article/russiagate-is-more-fiction-than-fact/.; Davis, "Trump, at Putin's Side, Questions U.S. Intelligence on 2016 Election."

[257] Gady and Austin, "Russia, The United States, And Cyber Diplomacy: Opening the Doors."

[258] Ibid.

[259] Argument is made by the US President Donald Trump

Furthermore, this attack happened in virtual space, meaning there was not any physical damage or casualties. If the US president was elected because of the interference, there is no way of knowing how much of an impact it had. It can be argued that even an analysis about the repercussions is only speculative. More so, there is no way of telling if there was any meaningful effect to begin with.[260]Furthermore, because the investigation is on-going and the US president himself is denying the allegation, it is hard to say whether and how Russian interference will affect future US cyber policy.

[260] Crowther, "National Defense and the Cyber Domain."

IV. Conclusion

Inter-state competition in cyberspace is aggressive and ongoing. Challenging states seek to undermine the global order to advantage their national interest. The US and Russia previously tried to begin dialogues on strengthening cybersecurity and limiting military use of cyberspace, as well as establishing stable international order and regulations such as rule of engagement in cyberspace in hopes of preventing future cyberwarfare. A report by the CSIS Commission on Cyberspace comments on the nature of the global digital environment: "The Internet is part town square (where people engage in politics and speech), part Main Street (where people shop), part dark alleys (where crime occurs), part secret corridors (where spies engage in economic and military espionage), and part battlefield."[261] Different perceptions between states are inevitable, and these can only be addressed through dialogue and compromise. Through dialogue and compromise, the US and Russia must develop shared international regulations and norms for its security in cyberspace to effectively work. However, these attempts have failed as the two states could not come to an agreement on their terms on cyberspace.

Recently, a Russian intelligence expert stated that the cyber war between the US and Russia has already begun. This awareness was already introduced in the 2015 US National Security Strategy. It showed that the world is already

[261] Whitehouse, "From Awareness to Action: A Cybersecurity Agenda for the 45th President."

in the process of cyberwarfare.[262] This cyberwarfare can start from an attack in cyberspace. To prevent such attacks, the US and Russia approach the problem of security in cyberspace from two different angles. The US pursues the freedom of information access and cross-border communication, the protection of personal privacy and intellectual property rights, and focuses on law enforcement at the domestic level with voluntary international collaboration.[263] Russia, on the other hand, insists that state sovereignty has to be recognized in cyberspace and focuses on developing binding international treaties and guidelines to control information access.[264] These fundamental differences between the two states have made it harder to create a policy that could limit competition in cyberspace.

Furthermore, according to the US, because most countries' security and economy have developed in a way that is deeply related to network infrastructure based on technology, cybercriminals and countries like Russia that oppose the global technological development are emerging as a big threat to the US.[265] In May 2015, *Newsweek* published an article, "Russia's Greatest Weapon May Be Its Hacker," stating that the US has identified Russia as the

---

[262] 「[RUSSIA 포커스] 가장 센 사이버전사 보유 러시아 전력 가장 위협적…중국은 과대평가된 듯」. 『중앙일보』, June 26, 2015, https://news.joins.com/article/18108558.; Kolomychenko, "On the Internet, Cyberwars Have Been Introduced [V Internet Vveli Kibervoyska]."

[263] 김상배. 「네트워크로 보는 세계정치의 변화: 사이버 안보와 디지털 공공외교를 중심으로」

[264] 장덕준, 「[이슈브리프] 러시아의 신안보이슈」.

[265] Clarke and Knake, *Cyber War*.

most potent challenger of the cyber war that has already begun, in which US assumes that Russia is responsible for numerous cyber attacks on the US government. Moreover, Russian hackers are referred to as prolific and outstanding cyber warriors that the US needs to prepare for accordingly.[266]

Russia, on the other hand, argues that the US has been purposely blocking Russia from rightfully competing against the US because the US wants to keep its hegemonic status in cyberspace. However, because the US-centric international order can potentially harm and threat Russia's national security, Russia fiercely and openly stated that it would do everything to achieve global governance in cyberspace. The difference in agenda also makes it harder to apply a policy of deterrence, as these two states do not have a shared understanding or mutual expectation of potential contingencies in cyberspace.

The main limitation of this analysis is that it lacks factual data from each state. Most of the evidence and various assertions are one-sided without feasible evidence. Furthermore, since this paper is the only a case study of the US-Russia cyber competition in the field of global governance, further studies should be done with respect to different aspects such as domestic policies, budgets, and actual instances of cyber conflict. Also, a similar study should be done on countries like Iran, North Korea, and China that have been recognized as the US' rivals in cyberspace, since Russia may not be the only country

[266] Matthews, "Russia's Greatest Weapon May Be Its Hackers."

competing against the US.

When the importance of cyberspace and its security arose, the US tried to contain and prevent possible competition and warfare by strategically using deterrence policy. However, the policy failed due to the unique nature of cyberspace that was not accounted for.[267] This led states such as the US and Russia look for different ways to prevent such competition. Yet, as aforementioned, fundamental differences in their approach to cyberspace led to a failure to compromise. Thus, the two states began to compete viciously in cyberspace to gain hegemonic status. The US and Russia have been competing to dominate the international order and global governance in cyberspace.[268] They have been militarizing cyberspace for defensive purposes. However, as the competition progressed, their defensive measures have become offensive measures. US cyber experts have stated that if such competition and cyber attacks continue, there soon will be a point where the US develops its cyber weapon in retaliation.[269] With the impact of Russian interference in the 2016 US election where the US sees it as an unforgivable attack on US national security and territory, one wonders if this marks the beginning of a US-Russian cyber war like one from the Cold War.

[267] Trujillo, "The Limits of Cyberspace Deterrence."
[268] Nocetti, "Contest and Conquest."
[269]Matthews, "Russia's Greatest Weapon May Be Its Hackers."

VI. Bibliography

"Assessing Russian Activities and Intentions in Recent US Elections." Intelligence Community Assessment, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Beckhusen, Robert. "The Russian Military Creates Its Own Cyber Troops." *War Is Boring* (blog), May 28, 2015. https://warisboring.com/the-russian-military-creates-its-own-cyber-troops/.

Benthem van den Bergh, Godfried van. "The Taming of the Great Nuclear Powers." *Carnegie Endowment for International Peace*, 2009, 20.

Blakeman, Bradley. "Cyber Warfare More Dire and Likely than Nuclear." The Hill, 27 2016. http://thehill.com/blogs/pundits-blog/technology/281475-cyber-warfare-more-dire-and-likely-than-nuclear.

Blue, Violet. "WCIT-12 Leak Shows Russia, China, Others Seek to Define 'Government-Controlled Internet.'" *ZDNet*, December 8, 2012. https://www.zdnet.com/article/wcit-12-leak-shows-russia-china-others-seek-to-define-government-controlled-internet/.

Borger, Julian, Luke Harding, and Miriam Elder David Smith in Johannesburg. "G20 Summits: Russia and Turkey React with Fury to Spying Revelations." *The Guardian*, June 17, 2013, sec. World news. http://www.theguardian.com/world/2013/jun/17/turkey-russia-g20-spying-gchq.

Boyd, Aaron. "DNI Clapper: Cyber Bigger Threat than Terrorism." *Federal Times*, February 4, 2016. https://www.federaltimes.com/management/2016/02/04/dni-clapper-cyber-bigger-threat-than-terrorism/.

Bronk, Christopher, and Dan Wallach. "Cyber Arms Control? Forget about It." *CNN*, March 26, 2013, International Edition. https://edition.cnn.com/2013/03/26/opinion/bronk-wallach-cyberwar/index.html.

Brunner, Elgin, and Manuel Suter. "Russia—Critical Sectors." In *An Inventory of 25 National and 7 International Critical Information Infrastructure*

Protection Policies, edited by Andreas Wenger, Victor Mauer, and Myriam Dunn. Zurich: Center for Security Studies, 2008. http://www.academia.edu/1606985/International_CIIP_Handbook_2008_2009_-_An_Inventory_of_25_National_and_7_International_Critical_Information_Infrastructure_Protection_Policies.

Builder, Carl H. "The Future of Nuclear Deterrence." Santa Monica: RAND Corporation, 1991. https://www.rand.org/pubs/papers/P7702.html.

Cerrudo, Cesar. "Why Cybersecurity Should Be The Biggest Concern Of 2017." *Forbes*, January 17, 2017. https://www.forbes.com/sites/forbestechcouncil/2017/01/17/why-cybersecurity-should-be-the-biggest-concern-of-2017/.

Chabrow, Eric. "Schmidt Meets with Russian Counterpart," July 2011. https://www.govinfosecurity.com/schmidt-meets-russian-counterpart-a-3841.

"China Asks U.S. to Explain Internet Surveillance." *Reuters*, June 17, 2013. https://www.reuters.com/article/us-usa-security-china/china-asks-u-s-to-explain-internet-surveillance-idUSBRE95G06R20130617.

Choucri, Nazli. *Cyberpolitics in International Relations*. MIT Press, 2012.

Ciolan, Ionela Maria. "Defining Cybersecurity as the Security Issue of the Twenty First Century. A Constructivist Approach." *The Public Administration and Social Policies Review* 5, no. 1 (2014): 17.

Clarke, Richard A., and Robert Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. Reprint edition. New York: Ecco, 2011.

"Competition in Cyberspace." *Armed Forces Journal*, January 1, 2013. http://armedforcesjournal.com/competition-in-cyberspace/.

Connell, Michael, and Sarah Vogler. "Russia's Approach to Cyber Warfare." CNA's Occasional Paper. CNA Analysis & Solution, March 2017. https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf.

"Convention on Cybercrime." European Treaty Series. Budapest: Council of Europe, 2001. https://www.coe.int/en/web/conventions/full-list.

Craig, A., and B. Valeriano. "Conceptualising Cyber Arms Races." In *2016 8th International Conference on Cyber Conflict (CyCon)*, 141–58, 2016. https://doi.org/10.1109/CYCON.2016.7529432.

Crowther, G. Alexander. "National Defense and the Cyber Domain." *The Heritage Foundation*, October 5, 2017, 83–97.

"Cyber Security Vs Information Security." *Hack2Secure* (blog), June 16, 2017. https://www.hack2secure.com/blogs/cyber-security-vs-information-security.

"Doctrine of Information Security of the Russian Federation [Doktrina Informatsionnoy Bezopasnosti Rossiyskoy Federatsii]." The Ministry of Foreign Affairs of the Russian Federation, December 5, 2016. http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.

Ell, Kellie. "FireEye CEO: If the US and Russia Had a Cyber War, Russia Would Win," March 15, 2018. https://www.cnbc.com/2018/03/15/fireeye-ceo-if-the-us-and-russia-had-a-cyber-war-russia-would-win.html.

"Fact Sheet: DHS 2008 End-of-Year Accomplishments." Department of Homeland Security, December 18, 2008. http://www.dhs.gov/xnews/releases/pr_1229609413187.shtm.

Feickert, Andrew. "The Unified Command Plan and Combatant Commands: Background and Issues for Congress," n.d.

Fischer, Eric A. "Cybersecurity Issues and Challenges: In Brief." Congressional Research Service, August 12, 2016.

Fitzpatrick, Alex. "U.S. Refuses to Sign UN Internet Treaty." *CNN*, December 14, 2012. https://edition.cnn.com/2012/12/14/tech/web/un-internet-treaty/index.html.

"Foreign Minister Sergey Lavrov's Interview with Amanpour Program on CNN International, Moscow, 12. October 2016," October 12, 2016.

The Ministry of Foreign Affairs of the Russian Federation. http://www.mid.ru/meropriyatiya_s_uchastiem_ministra/-/asset_publisher/xK1BhB2bUjd3/content/id/2497676.

Foxall, Andrew. “Putin’s Cyberwar: Russia’s Statecraft in the Fifth Domain.” Russian Studies Centre, May 2016. https://www.stratcomcoe.org/afoxall-putins-cyberwar-russias-statecraft-fifth-domain.

Gady, Franz-Stefan, and Greg Austin. “Russia, The United States, And Cyber Diplomacy: Opening the Doors.” EastWest Institute, 2010.

Gallagher, Sean. “US, Russia to Install ‘Cyber-Hotline’ to Prevent Accidental Cyberwar.” *Ars Technica*, June 18, 2013. https://arstechnica.com/information-technology/2013/06/us-russia-to-install-cyber-hotline-to-prevent-accidental-cyberwar/.

Gerson, Michael S. “Conventional Deterrence in the Second Nuclear Age:” Fort Belvoir, VA: Defense Technical Information Center, October 1, 2009. https://doi.org/10.21236/ADA510428.

Giles, Keir. “‘Information Troops’ - A Russian Cyber Command?” 1–16. CCD COE, 2011.

———. “Russia’s Public Stance on Cyberspace Issues.” In *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, 1–13. CCD COE, 2012.

Guertner, Gary L, Robert Haffa, and Geroge Quester. “Conventional Forces and the Future of Deterrence.” *Strategic Studies Institute, U.S. Army War College*, Strategic Concepts in National Military Strategy, March 5, 1992, 68.

Harvey, John. *Conventional Deterrence and National Security*. Fairbairn, A.C.T.: Air Power Studies Centre, 1997.

“Hillary Clinton’s Historic Speech on Global Internet Freedom,” January 2010. //2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

"How Does the Internet Fit into Russia's Security Strategy?" *Russia Direct*, May 4, 2016. http://www.russia-direct.org/company-news/how-does-internet-fit-russias-security-strategy?cv=1.

Ignatius, David. "Russia's Radical New Strategy for Information Warfare." *Washington Post*, January 18, 2017. https://www.washingtonpost.com/blogs/post-partisan/wp/2017/01/18/russias-radical-new-strategy-for-information-warfare/.

"International Forum 'Arctic - Territory of Dialogue' [Mezhdunarodnyy Forum «Arktika – Territoriya Dialoga»]." Kremlin. Accessed July 23, 2018. http://kremlin.ru/events/president/news/54149.

Jackson, William, and 2009 Jun 24. "DOD Creates Cyber Command as U.S. Strategic Command Subunit." *FCW*. Accessed July 23, 2018. https://fcw.com/articles/2009/06/24/dod-launches-cyber-command.aspx.

Johnson, David R., and David G. Post. "Law and Borders - the Rise of Law in Cyberspace." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, February 1, 1997. https://papers.ssrn.com/abstract=535.

Karnitschnig, Matthew. "NSA Flap Strains Ties With Europe." *Wall Street Journal*, February 9, 2014, sec. World. https://www.wsj.com/articles/wave-of-nsa-reports-strain-ties-with-europe-1391971428.

"Kaspersky: Russia Responds to US Ban on Software." *BBC News*, September 14, 2017, sec. US & Canada. https://www.bbc.co.uk/news/world-us-canada-41262049.

Kawasaki, Tsuyoshi. "Where Does Canada Fit in the US–China Strategic Competition across the Pacific?" *International Journal* 71, no. 2 (June 1, 2016): 214–30. https://doi.org/10.1177/0020702016643344.

Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 38, no. 2 (October 2013): 7–40. https://doi.org/10.1162/ISEC_a_00138.

Kissel, Richard. “Glossary of Key Information Security Terms.” National Institute of Standards and Technology, May 2013. https://doi.org/10.6028/NIST.IR.7298r2.

Klump, Ray. “Information Assurance vs. Cyber Security vs. Information Security: Clarifying the Differences | Faculty Forum.” *Lewis University Faculty Forum* (blog), January 6, 2018. https://www.lewisu.edu/experts/wordpress/index.php/information-assurance-vs-cyber-security-vs-information-security-clarifying-the-differences/.

Kolomychenko, Maria. “On the Internet, Cyberwars Have Been Introduced [V Internet Vveli Kibervoyska].” *Kommersant*, October 1, 2017. https://www.kommersant.ru/doc/3187320.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and National Security*. University of Nebraska Press, 2009. http://www.jstor.org/stable/j.ctt1djmhj1.

Kulikova, Alexandra. “The Contest of Rules: US, China, Russia Rival in Setting the Norms of Behavior in Cyberspace.” *Center for Global Communication Studies Mediawire* (blog), October 8, 2015. https://global.asc.upenn.edu/the-contest-of-rules-us-china-russia-rival-in-setting-the-norms-of-behavior-in-cyberspace/.

Laan, Marika Van. “ICANN, Russia, China, and Internet Reform: What You Need to Know.” *Ramen IR* (blog), October 23, 2016. https://ramenir.com/2016/10/23/icann-russia-china-and-internet-reform-what-you-need-to-know/.

Langevin, James R., Michael T. McCaul, Scott Charney, and Harry Raduege. “Securing Cyberspace for the 44th Presidency:” Fort Belvoir, VA: Defense Technical Information Center, December 1, 2008. https://doi.org/10.21236/ADA489361.

Lonsdale, David J. *The Nature of War in the Information Age: Clausewitzian Future*. Routledge, 2004. https://doi.org/10.4324/9780203508176.

Lowe, Christian, and Maria Kiselyova. “U.S. Says Concerned over Russia Blocking Access to LinkedIn.” *Reuters*, November 18, 2016. https://www.reuters.com/article/us-russia-linkedin-diplomacy/u-s-

concerned-over-russia-blocking-access-to-linkedin-ria-idUSKBN13D0ST.

Luhn, Alec, and Dan Roberts. “Obama Cancels Meeting with Putin over Snowden Asylum Tensions.” *The Guardian*, August 7, 2013, sec. US news. http://www.theguardian.com/world/2013/aug/07/obama-putin-talks-canceled-snowden.

Lunden, Ingrid. “LinkedIn Is Now Officially Blocked in Russia.” *TechCrunch*, November 17, 2016. https://techcrunch.com/2016/11/17/linkedin-is-now-officially-blocked-in-russia/.

Lyngaas, Sean. “Intel Chiefs Say Cyber Norms, Deterrence Strategy Still Elusive.” *FCW*, September 10, 2015. https://fcw.com/articles/2015/09/10/intel-cyber-norms.aspx.

MacFarquhar, Neil. “Russia Quietly Tightens Reins on Web With ‘Bloggers Law.’” *The New York Times* (blog), December 20, 2017. https://www.nytimes.com/2014/05/07/world/europe/russia-quietly-tightens-reins-on-web-with-bloggers-law.html.

Markoff, John, and Andrew E. Kramer. “U.S. and Russia Differ on a Treaty for Cyberspace.” *The New York Times*, June 27, 2009, sec. World. https://www.nytimes.com/2009/06/28/world/28cyber.html.

Mate, Aaron. “Russiagate Is More Fiction Than Fact.” *The Nation*, 2017. https://www.thenation.com/article/russiagate-is-more-fiction-than-fact/.

Matthews, Owen. “Russia’s Greatest Weapon May Be Its Hackers.” *Newsweek*, May 7, 2015. https://www.newsweek.com/2015/05/15/russias-greatest-weapon-may-be-its-hackers-328864.html.

Maurer, Tim, and Robert Morgus. “Compilation of Existing Cybersecurity and Information Security Related Definitions.” New America Foundation, October 2014.

McConnell, Bruce W, Pavel Sharikov, and Maria Smekalova. “Suggestions on Russia-U.S. Cooperation in Cybersecurity.” Russian International Affairs Council and EastWest Institute, May 11, 2017. http://russiancouncil.ru/en/activity/policybriefs/suggestions-on-russia-u-s-cooperation-in-cybersecurity/.

Medvedev, Sergei A. “Offense-Defense Theory Analysis of Russian Cyber Capability.” Naval Postgraduate School, 2015. http://calhoun.nps.edu/handle/10945/45225.

Modestov, Sergei. “The Space of Future War [Prostranstvo Budushchey Voyny].” *Bulletin of the Academy of Military Science*, no. 2 (2003).

Morgan, Patrick. “Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm.” In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, 2010. https://doi.org/10.17226/12997.

“National Cyber Defense Strategy.” Department of Defense, April 2015. https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

Nocetti, Julien. “Contest and Conquest: Russia and Global Internet Governance.” *International Affairs* 91, no. 1 (January 2015): 111–30. https://doi.org/10.1111/1468-2346.12189.

———. “Russia’s ‘dictatorship-of-the-Law’ Approach to Internet Policy.” *Internet Policy Review* 4, no. 4 (November 10, 2015): 19.

Nye, Joseph S. “Nuclear Lessons for Cyber Security:” Fort Belvoir, VA: Defense Technical Information Center, January 1, 2011. https://doi.org/10.21236/ADA553620.

Phneah, Ellyne. “Cyber Warfare Not Theoretical, Can Actually Kill.” *ZDNet*, November 17, 2011. https://www.zdnet.com/article/cyber-warfare-not-theoretical-can-actually-kill/.

Polantz, Katelyn, and Stephen Collinson. “Mueller Probe: 12 Russians Indicted for DNC Hack.” *CNN*, July 14, 2018. https://edition.cnn.com/2018/07/13/politics/russia-investigation-indictments/index.html.

Pont, George du. “Criminalization of True Anonymity in Cyberspace, The.” *Michigan Telecommunications and Technology Law Review* 7, no. 1 (2011): 27.

Powell, Robert. “Nuclear Deterrence Theory, Nuclear Proliferation, and National Missile Defense.” *International Security* 27, no. 4 (April 2003): 86–118. https://doi.org/10.1162/016228803321951108.

“Putin Invited BRICS Countries to Conclude an Agreement on Information Security [Putin Predlozhil Stranam BRIKS Zaklyuchit’ Soglasheniye Po Informatsionnoy Bezopasnosti].” *TASS*, September 1, 2017. http://tass.ru/politika/4523253.

Reardon, Robert, and Nazli Choucri. “The Role of Cyberspace in International Relations: A View of the Literature,” 1:34. San Diego, 2012.

Rid, Thomas. “All Signs Point to Russia Being Behind the DNC Hack.” Motherboard, July 25, 2016. https://motherboard.vice.com/en_us/article/4xa5g9/all-signs-point-to-russia-being-behind-the-dnc-hack.

Rollins, John, and Anna C. Henning. “Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations.” Congressional Research Service, March 10, 2009. https://fas.org/sgp/crs/natsec/R40427.pdf.

“Russia.” Freedom House, October 27, 2015. https://freedomhouse.org/report/freedom-net/2015/russia.

“Russia Moves toward Creation of an Independent Internet.” *DW.COM*, January 17, 2018. https://www.dw.com/en/russia-moves-toward-creation-of-an-independent-internet/a-42172902.

“Russia Must Effectively Respond to Cyber Threats, Putin Said [Rossiya Dolzhna Effektivno Reagirovat’ Na Kiberugrozy, Zayavil Putin].” *RIA Novosti*, July 5, 2013. https://ria.ru/defense_safety/20130705/947885730.html.

“Sands: Ban on Kaspersky Programs in the US Violates the Rules of Trade [Peskov: Zapret Na Programmy ‘Kasperskogo’ v SSHA Narushayet Pravila Torgovli].” *RIA Novosti*, September 14, 2017. https://ria.ru/world/20170914/1504774900.html.

Satter, Raphael, Jeff Donn, and Chad Day. “Inside Story: How Russians Hacked the Democrats’ Emails.” *US News & World Report*, November

6, 2017. https://www.usnews.com/news/world/articles/2017-11-03/inside-story-how-russians-hacked-the-democrats-emails.

Sharikov, Pasha. "Cybersecurity in Russian-U.S. Relations." CISSM Policy Brief. Center for International Security Studies at Maryland, April 2013. http://www.cissm.umd.edu/publications/cybersecurity-russian-us-relations-0.

Sharikov, Pavel. "U.S.-Russia Relations in the Sphere of Information Security." Carnegie Moscow Center, November 1, 2013. https://carnegie.ru/2013/11/01/u.s.-russia-relations-in-sphere-of-information-security-pub-63163.

Singh, Aniruddha, Abhishek Vaish, and Pankaj Kumar Keserwani. "Information Security: Components and Techniques." *International Journal of Advanced Research in Computer Science and Software Engineering* 4, no. 1 (2014): 6.

Smith, Julianne, and Adam Twardowski. "The Future of U.S.-Russia Relations." Strategy & Statecraft. Center for New American Security, January 2017. https://www.cnas.org/publications/reports/the-future-of-u-s-russia-relations.

Softa, Jan. *Threats Against Russia's Information Society*. BookSurge Publishing, 2008.

Sottek, T. C. "Everything You Need to Know about PRISM." The Verge, July 17, 2013. https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet.

"Statement by Secretary Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector | Homeland Security." Homeland Security, 2017. https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

Stevens, Melissa. "Cybersecurity Vs. Information Security: Is There A Difference?" *BitSight* (blog), March 15, 2016. https://www.bitsighttech.com/blog/cybersecurity-vs-information-security.

Stewart, Phil, and Valerie Volcovici. "Trump Backtracks on Cyber Unit with Russia after Harsh Criticism." *Reuters*, July 9, 2017.

https://www.reuters.com/article/us-usa-trump-russia-cyber/trump-backtracks-on-cyber-unit-with-russia-after-harsh-criticism-idUSKBN19U0P4.

The White House. “Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,” 2009, 76.

———. “FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security,” June 17, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol.

———. “International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World,” 2011. https://doi.org/10.1037/e688502011-001.

———. “Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” May 11, 2017. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

———. “Statement by President Donald J. Trump on the Elevation of Cyber Command.” The White House, August 18, 2017. https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/.

Trujillo, Clorinda. “The Limits of Cyberspace Deterrence.” *National Defense University Press* Joint Force Quarterly, no. 75 (2014): 10.

“Ukraine Crisis: Obama Rules Out Military Action.” *The Associated Press*, August 28, 2014. https://www.cbc.ca/news/world/ukraine-crisis-obama-rules-out-military-action-1.2749066.

“U.S. Strategic Command: Factsheets.” U.S. Strategic Command. Accessed July 23, 2018. http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/.

Vingoe, Sandy. “Cybersecurity and the Ukraine Crisis: The New Face of Conflict in the Information Age.” NAOC, June 19, 2015.

http://natoassociation.ca/cybersecurity-and-the-ukraine-crisis-the-new-face-of-conflict-in-the-information-age/.

Volz, Dustin. “Microsoft President Brad Smith Calls for a ‘Digital Geneva Convention’ in the Wake of the DNC Hacking Scandal.” *Business Insider*, February 14, 2017. http://www.businessinsider.com/r-digital-geneva-convention-needed-to-deter-nation-state-hacking-microsoft-president-2017-2.

Waltz, Kenneth N. “Nuclear Myths and Political Realities.” *The American Political Science Review* 84, no. 3 (September 1990): 731. https://doi.org/10.2307/1962764.

Ward, Alex. “‘It’s Probably Going to Get Worse’: A Former Top Intel Official on Russia Election Meddling.” Vox, February 27, 2018. https://www.vox.com/world/2018/2/27/17046300/russia-election-meddling-hack-treverton-interview.

Ware, Doug G. “NATO Officially Recognizes Cyberspace as Domain for War.” *UPI*, June 14, 2016. https://www.upi.com/NATO-officially-recognizes-cyberspace-as-domain-for-war/2271465941545/.

“What Does ICANN Do?” ICANN. Accessed July 23, 2018. https://www.icann.org/resources/pages/what-2012-02-25-en.

“What Is Cyberspace? Examining Its Characteristics.” *Air Power Development Centre* Pathfinder, no. 157 (June 2011).

“Whitehouse - From Awareness to Action A Cybersecurity Agenda f.Pdf.” Accessed July 23, 2018. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170110_Lewis_CyberRecommendationsNextAdministration_Web.pdf.

Whitehouse, Sheldon. “From Awareness to Action: A Cybersecurity Agenda for the 45th President,” January 2017, 34.

Xu, Longdi. “Cyberspace Security: Trends, Conflicts and Strategic Stability.” China Institute of International Studies, November 10, 2017. http://www.ciis.org.cn/english/2017-11/10/content_40064730.htm.

김상배. 「네트워크로 보는 세계정치의 변화: 사이버 안보와 디지털 공공외교를 중심으로」. 제주평화연구원, 2012.

———.「 세계 주요국의 사이버 안보 전략: 비교 국가전략론의 시각」. 국제지역연구, 2017: 67-108. http://snuiis.re.kr/sub5/5_3.

———.『버추얼 창과 그물망 방패』. 서울: 한울아카데미, 2018. http://www.kyobobook.co.kr/redi_book.jsp?b=9788946070516&g=KOR.

성기노. 「세계 최초의 사이버 전쟁과 사이버안보법」. 『보안뉴스』, February 5, 2017. http://www.boannews.com/media/view.asp?idx=53325.

신범식. 「러시아의 사이버 안보의 전략과 외교」. In 『사이버 안보의 국가전략: 국제정치학의 시각』, 397. 5. 서울: 사회평론아카데미, 2017.

신성호. 「미국의 사이버 안보 전략과 외교」. In 『사이버 안보의 국가전략』: 국제정치학의 시각, 397. 2. 서울: 사회평론아카데미, 2017.

장덕준. 「[이슈브리프] 러시아의 신안보이슈」. 『국내 5 대 협력연구기관 공동기획』. 여시재, December 6, 2017. https://www.yeosijae.org/posts/356?project_id=2&topic_id=2.

페트로바 아나스타시야. 「'뒤늦은 양병(養兵)'...러시아도 올해 안에 사이버 부대 창설」. 『*Russia Beyond*』, 18 2013. https://kr.rbth.com/military_and_tech/2013/07/18/42527.

「[RUSSIA 포커스] 가장 센 사이버전사 보유 러시아 전력 가장 위협적…중국은 과대 평가된 듯」. 『중앙일보』, June 26, 2015, https://news.joins.com/article/18108558

ABSTRACT (Korean)

신 미러 경쟁: 미국과 러시아 간의 사이버 전략 경쟁 분석

이 논문은 미국과 러시아의 사이버 공간에서의 경쟁이 세계적인 지배력을 획득하기위한 헤게모니 경쟁이라고 주장한다. 사이버 전문가들은 현재 사이버 전쟁이 임박한 상황이고 만약 전쟁이 일어난다면 핵전쟁보다 더 파괴적일 것이며, 따라서 사이버 전쟁을 방지해야 한다고 말한다. 핵전쟁을 성공적으로 막은 억제론(Deterrence)이 사이버 전쟁을 방지하기 위한 수단으로 제안 되었으나, 사이버 공간의 특성상 억제론은 효과가 없다. 이 때문에 미국과 러시아를 포함한 국가들이 사이버 전쟁을 방지하기 위하여 협력을 시도하였으나, 사이버 규범에 대한 보편적인 정의와 이해가 없기 때문에 국가들은 사이버 공간을 다르게 이해하고 해석하고 접근한다.

미국은 사이버 공간에서의 사이버안보와 정보의 자유로운 흐름을 추구하는 반면 러시아는 정보 안보과 국가 주권을 추구한다. 따라서 이 논문은 억제론이 가상 현실과 익명성이라는 사이버 공간의 고유한 특성으로 인해 기존의 영역과는 다른 사이버 공간에서의 갈등을 예방하는 데는 효과가 없다고 주장한다. 미국과 러시아는 억제론의 결여로 인해 사이버 공간에서 갈등을 막기위한 대안을 모색을 하였지만, 이 또한 사이버 공간에 대한 근본적으로 다른 인식으로 인해 실패하였다고 주장한다. 그로인해 미국과 러시아가 사이버 공간에서 헤게모니 지위를 놓고 경쟁을 시작하였다 주장한다.