Univerzita Karlova

Fakulta sociálních věd

Institut politologických studií

Diploma thesis project

Beyond the Impasse: Prospects for Joint Cooperation between Russia and the US in Counter Cyberterrorism

Name: Kledian Myftari

Academic Advisor: Vitek Střitecky, Ph.D.

Study Programme: Master’s in International Security Studies (MISS)

Year of Submission: 2021

TABLE OF CONTENTS

ABSTRACT

Russia and the US have both articulated their willingness to develop a regime for counter cyberterrorism. Yet, to date, they have been unsuccessful in following through with this goal. Their failure to form such a regime can best be explained through the lens of social constructivism, and most specifically, through the concept of strategic culture, given that such an approach allows for the examination of ideological, historical, and cultural issues that have shaped the strategy choices of both countries. Russia and the US have successfully formed regimes with other countries in which issues of counter cyberterrorism come to play. Russia has entered into agreements with BRICS and with the Shanghai Cooperation Organization. The US has involved itself in cybersecurity regimes both with its NATO allies and with its Latin American and Caribbean allies. Russia and the US have furthermore entered into a number of agreements with each other, including the Anti-Ballistic Missile Treaty, the Intermediate-Range Nuclear Forces Treaty, and New-START. A strategic culture perspective, which focuses primarily on historical factors, such as a history of invasion or lack thereof, and the relations of both countries with their respective neighbors, reveals how the discourse of human rights and the freedoms of expression and access to information have informed the prospective of the formation of a counter cyberterrorism regime differently than is the case with treaties concerning, for instance, nuclear issues. Moreover, recent historical events have fomented increasing distrust between the two nations. What is necessary, in this case, is the development of a culture of trust between Russia and the US. This will be best achieved through one-and-one-half or two-track diplomacy.

Key words: Counter Cyberterrorism, Cybersecurity, Regime Formation, Trust, Track One-and-a-Half Diplomacy, Track Two Diplomacy

INTRODUCTION

On 2 September 1998, the presidents of Russia and the US reaffirmed that the two nations are “natural partners in advancing international peace and stability” and that they “have devoted particular attention to intensifying joint efforts to eliminate threats inherited from ‘the Cold War and to meet common security challenges at the threshold of the twenty-first century” (William J. Clinton and Boris Yeltsin 1998, p. 505). The joint statement issued by the presidents of Russia and the US focuses on such threats as weapons of mass destruction, be they nuclear, chemical, or biological, and articulates that what is at stake is not only the security of the two signatories, but also of the global community at large. Although the Statement fails to mention the issues of cyberwarfare or cyberterrorism, it specifically mentions the cyberworld, “recognizing the importance of promoting the positive aspects and mitigating the negative aspects of the information technology revolution […] to assure the future strategic security interests of our two countries” (p. 506). The document refers to the productive discussions the two countries had had within the framework of the US Department of Defense Consultative Group concerning the potential issues posed by the advent of the year 2000, and additionally stresses that the US and Russia had committed to further studying this potential threat (pp. 506-507). The Statement further articulates the need for the mobilization of the entire international community in countering such threats. It concludes with Russia and the US committing to continually playing “a leadership role bilaterally and multilaterally to advance common objectives in the area of security” (p. 507), The Joint Statement’s discussion of the problem of cybersecurity was thus limited to what was known as the “Y2K Bug” and failed to deal with other cyberthreats more directly. Other cooperative efforts between Russia and the US in Counter Cyberterrorism have been notably rare or have proven to be highly unsuccessful.

Terrorism and Cyberterrorism

Traditionally, terrorism has been identified with attacks on spaces where many people are concentrated—the Moscow or London subways, the commuter railway of Madrid, or a trendy restaurant in Paris. Terrorist attacks have served a primarily political agenda. Although contemporary media discourse may tend to conflate terrorism with the Middle East, one need only look back a few decades at West Germany's Red Army Faction, more commonly known as the Bader-Meinhof gang, whose operations ushered in the German Autumn of 1977.[1] Somewhat more recently, the Euskadi ta Askatasuna (ETA), a leftist Basque nationalist and separatist organization, left over 800 people dead in Spain.[2] Even today, the US deals with a rise of domestic terrorism with White Supremacist groups becoming emboldened by the (former) Trump administration. The 6 January 2021 occupation of the US Capitol building by ardent Trump supporters has been deemed, in a testimony presented by the Director of the FBI, Christopher Wray, to the US Senate Judiciary Committee, an act of domestic terrorism, (Ryan Lucas 2021). From the 1980s onward, the realm of terrorism discovered a new playing field. Not only were terrorist acts likely to be perpetrated on physical spaces, but they were also seen to be plausible on another turf—that of cyberspace. As will be explored in Chapter I, an exact definition of cyberterrorism is elusive. Distinctions must be made between this potential threat and other forms of cybercrime, and it must be separated from the phenomenon of cyberwarfare. Given that the cyberworld is a new domain, its scope, use, and misuse are still being defined. Moreover, its complexities are in a constant state of transformation and redefinition. Of particular concern is the issue of just who the perpetrators are. The latter will prove to be one of the critical issues that distinguish cyberterrorism from cyberwarfare.

The term "cyberterrorism" first coined in the 1980s by Barry C. Collin of the then Palo Alto-based Institute for Security and Intelligence (Doris E. Denning 1999, p. 281). Although it is frequently cited in retrospect, Collin's definition held very little currency at the time. It was not until the early 1990s that it became widely accepted that the rapid expansion of the Internet came with specific risks. Over the decade, the notion of cyberterrorism grew. In 1996, Collin presented remarks at the 11th International Symposium for Criminal Justice Issues, which were published the following year. Collin foregrounded the strong possibility of a terrorist attack capable of disrupting or altering such processes as air traffic control; financial transactions; the manufacturing of pharmaceuticals, utility systems, etc. Bombs could be placed around a city, receive information from each other, and be programmed to detonate simultaneously. For Collin, the realistic threat of cyberterrorism was unfolding in an uncharted domain, the convergence of the physical and virtual worlds. (Barry E. Collin, 1997, p. 15). In 1996, John Deutsch, the former director of the CIA, testified before the US Senate Permanent Subcommittee on Investigations as to the capability of terrorist groups to attack the information infostructure of the US. In his statement, Deutsch stressed the knowledge of the Internet held by such groups who had increasingly used technology for their communications. Deutsch specifically mentioned the Lebanese Hezbollah, and lesser-known cells such as the one responsible for the 1993 attack on the World Trade Center (John Deutsch 1996). The following year, Deutsch presented an address at Tel Aviv University in which he argued that, due to the cyber realm, terrorism now needed to be fought more strongly than in the past. To this effect, he argued for international cooperation (Harris, David, 1997, p. 1).

The US government came to recognize the implications of cyberterrorism formally. In February 2004, a hearing entitled "Virtual Threat, Real Threat: Cyberterrorism in the 21st Century" was held before the US Senate Subcommittee on Terrorism, Technology, and Homeland Security. James Lourdeau, Deputy Assistant Director of the FBI, assessed the growing possibility serious of cyberterrorist attacks. He stressed that although, to date, cyberattacks by terrorists or persons affiliated with terrorist cause had been limited to unsophisticated effortd (such as email bombings or the publication of threatening content), terrorist groups, nonetheless, were becoming capable of network-based attacks. They were likely to become able to acquire the skills needed for a major cyberterrorist event (James Lourdeau, 2004, p. 7). Lourdeau further stresses that the FBI fully recognized the growing threat of cyberterrorism since terror groups would either develop or hire hackers to complement large physical attacks with cyberattacks (James Lourdeau 2004, p. 7).

Despite the substantial policy and academic discourse on cyberterrorism that has appeared in the US over the past 30 years, the concept is far less discussed in Russia. This distinction will be a significant component of the contrastive study of the US and Russia's discourse on cyberterrorism and will constitute a major thread that will run through the remainder of the thesis. As an introduction to Russia's conceptualization of this phenomenon, a brief examination of the notion of "cyber" as it appears in Russian strategic and political discourse is in order here. A 2018 CNA study by Michael Connell and Sarah Vogler explains that, while discussing warfare, Russians rarely use the terms *kiber* (cyber) or *kibervoyna* (cyberwarfare) unless they are referring to foreign texts on the subject. Instead, they view the cyber potential in warfare as an integral part of a broader holistic concept that includes computer network operations, electronic warfare, psychological operations, and information operations, all intended to provide a mechanism that allows the state to dominate the information landscape and be deployed along with other strategies of war (2018, p. 3). Russia relies upon information warfare to achieve political objectives without deploying traditional military strategies (Michael Connell and Sarah Vogler 2018, p, 5). The term cyberwarfare in and of itself has very little currency in Russia. To the international community, Russia is perceived primarily as a perpetrator of cyberattacks rather than as a victim. One need only consider its purported attacks on Estonia (2007), Ukraine (2014), and Georgia (2020). Most famously, it was accused of attacks against the Democratic Party during the 2016 US elections. In Western eyes, these allegations have overshadowed Russia's vulnerability to cyberterrorism on its turf. Despite the sparse discussions on the counter cyberterrorism efforts underway on the domestic level, there are several international efforts to this effect in which Russia has taken part.

Russia, the US, and Counter Cyberterrorism

Despite the laudable intentions of cooperation between Russia and the US in cybersecurity embedded into the two countries' 1998 joint statement, very few tangible results have been witnessed since the signing of the document. In 2000, President Vladimir Putin signed into effect Russia's *Information Security Doctrine of the Russian Federation*, which recognized a deterioration in the security of data regarding state secrets. This decline was due in part to a brain drain in which the majority of experts in the field had emigrated away from Russia, forcing the country to purchase foreign equipment that could eventually be breached by outside sources[3]. Moreover, resources and funding to protect Russia from such threats were scant. One of the cyberthreats mentioned in the Doctrine which originate abroad is those posed by terrorist organizations. Cyberterrorist threats stemming from within the Russian Federation are not mentioned (Ministry of Foreign Affairs of the Russian Federation 2000).

The previous efforts of the Defense Consultative Group were promising, and the participants worked together to prevent a Y2K missile launch. Russia and the US later successfully collaborated in the encryption of the Moscow-Washington hotline. Nonetheless, cooperative efforts broke down on a number of levels. In 2001, the Council of Europe opened its *Convention on Cyber Crime* up for international signatures. The Convention was intended to address a number of categories of crimes committed via the Internet. The US became a signatory of this Convention while Russia did not. In contrast, in 2006, Russia, as chair of the G8 introduced an initiative fostering public-private partnerships designed to counter organized crime and terrorism. Cybersecurity was one of the primary domains covered by the initiative.

Although both the US government and private US corporations took part in the initiative, the effort has led to a scant number of concrete results.

From the perspective of Russia and the US, despite the countries' 1998 declaration of intent to provide leadership in global efforts to counter cyberterrorism, any cooperation to this effect between the two countries has not come to fruition. Were the two superpowers to work together to counter cyberterrorism, the consequences would affect favorably their own security, and enhance cybersecurity on a global level. It is the purpose of this thesis to examine the events and postures that have caused impasses for the creation of a joint cybersecurity regime between Russia and the US to counter eventual cyberterrorist attacks and to explore how meaningful and fruitful cooperation could be developed.

Structure, Theory, and Methods of this Thesis

The following discussion will be divided into five chapters. Chapter I will be devoted to the existing status of the field. It will explore the complexity of cyberterrorism and explore why there has been considerable difficulty in arriving at the definition of the phenomenon. It will explore the history of political discourse and criticism on cyberterrorism, looking back to the 1980s, when the term was first coined and focusing on the 1990s and early years of the new millennium when it gained currency. A review of existing scholarly and policy literature will then ensue, and it will be made clear that there has been little if any work to date completed on the difficulties that Russia and the US have had in creating a regime to fight cyberterrorism. Chapter II will establish the theoretical premises on which the study will draw. In general terms, the thesis will follow a Social Constructivist approach. It will further be mediated by the concept of Strategic Culture, which although frequently employed to examine the use of force in a conflict, can be reconceived to explore the tendencies of the two super powers to engage in or avoid engaging in the development of a counter cyberterrorism regime. Combined, these two theoretical approaches offer a framework in which less-tangible stances and historical factors can be untangled. Chapter III will explore how both Russia and the US have become involved in other regimes, which in part fight cyberterrorism. These include Russia's membership in the Shanghai Cooperation Organization and its efforts with the BRICS group in cybersecurity and the US's cooperation to this effect with the EU and Latin America. It will further foreground other areas in which, other than the domain of counter cyberterrorism, Russia and the US have successfully entered cooperation. Chapter IV will explore where attempts made by the two nations to collectively counter cyberterrorism have failed. It will examine the stances, ideological approaches, historical processes, and other factors that have rendered difficult the development of a counter cyberterrorism regime between Russia and the US. Chapter V will analyze both successes and impediments in accordance with the framework of Strategic Culture. The conclusion will offer a forward look at how Russia and the US could come together to overcome the hindrances that have prevented the development of a counter cyberterrorism regime.

Research Questions and Hypotheses

The primary research question that propels this thesis is why Russia and the US have failed to form a counter terrorism regime, despite the expression of good will on the part of both parties to enter into such an agreement. The following hypotheses have been identified, and will be examined through the constructivist lens of Strategic Culture:

1) The positions of Russia and the US regarding the possibility of cooperation are determined to a large extent by their diverse ways of defining and approaching the notion of cyberspace. (This notion draws, in part, upon the work of Franz-Stefan Gady and Greg Austin, 2009).

2) Issues of human rights and open societies, which bring to bear upon the notion of cyberterrorism, are characteristic of Western discourse, and hence are, by nature, distasteful to Russia.

3) The US is reluctant to enter into any agreement that is inimical to its worldwide economic issues, and hance, is unwilling to negotiate its stance.[4]

5) Cooperation will be most likely fostered through Track II diplomacy.

As will be demonstrated in the literature review in Chapter I, several studies have begun to approach this or similar topics. Yet, to date, there has been no study which explores from a diverse perspective the failure of Russia and the US to develop a counter cyberterrorism regime. This analysis will be the primary contribution of this ongoing discussions of the participation of the two superpowers in international cybersecurity.

CHAPTER I

STATUS OF THE FIELD: DEFINITIONS, HISTORICAL PERSPECTIVES, AND BRIEF LITERATURE REVIEW

The realm of cybersecurity has been described in a Fraser Report as “the new Wild West […] where the arm of international law has not yet arrived” (Alexander Noens, Seychelle Cushing, and Alan W. Dowd 2018, p. 7). The report foregrounds the dearth of security regimes, despite multiple calls for “norms and standards regarding the use of cyber space and cyber security” (2018, p. 7). If cybersecurity is deemed uncharted territory for international law, then the sub-domain of counter cyberterrorism must be even more unmapped in that the very definition of the threat remains in flux. Referring to Russia and China’s failure to sign the 2004 Budapest Convention on Cybercrime, the Council on Foreign Relations argues that an effective cyber regime only works if all major powers subscribe to it and accept its provisions. The Council asserts that either the Budapest Convention needs to be adopted to attract more participants, or there is need for a new treaty altogether. It further stresses that such efforts would be most effective if they received a mandate from the UN General Assembly to develop a universal convention based on the Budapest Convention or alternative proposals already in existence (Council on Foreign Relations 2018).

The notion of cyberterrorism falls under the general rubric of cybercrime, and is related to, but distinct from cyberwarfare. Although there have been numerous cyberattacks perpetrated by governments and individuals, an actual cyberterrorist attack is at this point hypothetical. Nonetheless, it must be considered a very real possibility. In a 2003 assessment of the threat of cyberterrorism, James F. Pasley looks back at 9/11 when it was unclear just how many jets had been hijacked and where they were headed. The US’ Federal Aviation Administration (FAA) knew the exact location of all commercial aircrafts in the air. Describing the potential effect if these attacks had been combined with a cyberattack, Pasley asserts that had the terrorists been able to attack the digital structure of the US by disabling the FAA's computers or by reprogramming its information, the 9/11 attacks could have been much worse (James F. Pasley 2004, p. 404).

The internet is highly attractive to terrorists for a number of reasons. A paper presented by Murat Dogrul, Adil Aslan, and Eyyp Celik at the 3rd International Conference on Cyber Conflict in Tallinn, Estonia in 2011 articulates the main advantages offered to terrorists by the internet. First of all, it is inexpensive to use. Terrorist groups can make do with fewer people and less funding.[5] They can target and affect large numbers of people with a fixed budget. In other words, there is an extremely high cost-benefit ratio. Secondly, the internet offers anonymity, inasmuch as terrorists can be a long way away from their targets. No longer is it necessary for terrorists to establish themselves in a country with a weak government. Thirdly, the internet targets are poorly protected. This weakness facilitates the speed and form of the attacks, given that the terrorist act is not contingent upon the connection speed of the attacker. In contrast, the connection speed of the victim can be used to the attacker's advantage. Dogrul, Aslan, and Celik argue that an ideal strategy for terrorists would be a combination of physical and cyberattacks. They note, moreover, that terrorist groups are making an increased use of information technology to raise and launder funds; develop plans; spread propaganda; communicate internally; share knowledge and information with affinitive groups; command and control; undertake research and development; generate international support; recruit members, and gather intelligence. The authors stress that, together with the above advantages, the internet offers little or no regulation, potentially huge audiences, and the anonymity of communication (2011, pp. 32-33). The internet, by extension, could easily be employed to undertake other phases of an attack.

Definitions and Historical Perspective of the Notion of Cyberterrorism

In 1991, the US National Academy of Sciences published a report arguing that the virtual world held ominous possibilities. The report on computer security stresses that since the US depends on computers, it must be recognized that these machines are vulnerable due to poor design, insufficient quality control, accidents, and most alarmingly, to deliberate attack. It argued that future thieves may well be able to do more damage with a keyboard than with a bomb (National Academy of Sciences 1991, p. 7).

The concept of cyberterrorism continued to grow in importance during the period leading up to the new millennium. Fears were mounting as the world approached Y2K. The mere notion that a computer glitch entailing the confusion of the year 2000 with 1900 which would cause planes to tumble from the sky and financial records to be destroyed was almost as entertaining as it was frightening. The millennium glitch quickly became entrenched in popular culture, US television shows, such as *The Simpsons* and *Family Guy* presented apocalyptic Y2K episodes, and the last months of 1999 saw a wave of pop songs taking a humorous or ironic look at the upcoming calamity. Jim Infantino, a Boston-based songwriter and bandleader who released the tune “Y2K Hooray,” would later write of the experience in hindsight, explaining that people were beginning to question if computer-enhanced living was worth it. Infantino stressed that the lead-up to the new millennium felt as if society were entering a science fiction chapter in the life of humanity. Despite all concerns, it turned out, Y2K was just another year (David Buck 2017).

Together with the pop-culture hype that the potential Y2K catastrophe had generated was an official US government response. Project Megiddo, whose name was derived from a hill in northern Israel key to the biblical notion of Armageddon, was established by the FBI to assess the threat of terrorism that accompanied the advent of the new millennium. Although the actual turn of the millennium would occur on 1 January 2001, the Project Megiddo report released on 20 October 1999 indicates that the real danger was associated with the start of the year 2000, which had come to have special meaning for many fringe groups. The report focuses, in part, on extremist Christian religious groups associated with white supremacy and antisemitism, and especially those who desired to counter a war against the white race (Federal Bureau of Investigation 1999, p. 10). Together with religious fanaticism was the prevalence of a conspiracy theory involving the establishment of a New World Order (NWO), or one-world government, whose adherents believed that the computer breakdown which would occur on 1 January 2000 would cause social, economic, and political chaos in the US. In turn, a situation would be exploited by the UN to forcibly take control of the country and provide a catalyst for the birth of the NWO (Federal Bureau of Investigation, 1999, p. 11). Although Project Megiddo did not specifically mention the potential use of cyberspace in a Y2K-related terrorist attack, it did foreground the convergence of fringe religious and political groups, Y2K, and terrorist activity.

The US government has attempted to define cyberterrorism, relying heavily on academic approaches to the topic. For instance, the FBI defines cyberterrorism as a "premeditated, politically motivated attack against information, computer systems, computer programs and data which results in violence against noncombatant targets by sub national groups or clandestine agents" (Yemi Faleti 2018). This exact definition has been attributed by Maura Conway to Mark M. Pollitt.[6] A more thorough and all-encompassing definition of cyberterrorism was offered by Dorothy Denning in a May 2000 testimony before the US House of Representatives Armed Forces Committee. Denning defines the phenomenon as follows:

> Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people to furtherance political or social objectives. Further, to qualify as cyberterrorism, an attack should

> result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not. (Dorothy Denning 2000, cited in Maura Conway, 2012, p. 285).

Denning later further clarified her definition, attempting to better distinguish it from other types of cybercrime, adding the following caveat to her discussion:

> To fall in the domain of cyberterror, a cyberattack should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism, and it must be conducted for political and social reasons. Critical infrastructures are likely targets. Attacks against these infrastructures that lead to death or bodily injury, extended power outages, plane crashes, water contamination, or billion-dollar banking losses would be examples (2006, p. 125).

James F. Pasley has provided significant details as to what a cyberterrorist attack could entail. For Pasley, a cyberterrorist attack is unlikely to occur separate from other terrorist attacks. On the contrary, it is most likely to occur in tandem with other acts of terror. Pasley identifies four forms that a cyberterrorist attack could assume: 1) web displacement, 2) domain name service attacks; 3) distributed denial of service attacks, and 4) worms. He defines these four categories and breaks them down further. A web displacement can entail both overt and semantic attacks. An overt attack changes the content of a website to display pro-terrorist propaganda. A semantic attack, which Pasley feels is more dangerous, makes subtle alterations, which “could lead to faulty decision-making with potentially disastrous results” (2003, p. 405). Like web displacement attacks, Domain Name Service (DNS) attacks “provide false information in the guise of a legitimate source” (2003, p. 405), but this time by funneling website seekers to different addresses. Distributed Denial of Service (DDS) attacks involve the victimization and overwhelming of computers with data, thereby shutting down sites (2003, p. 405). Finally, worms burrow inside a computer to disrupt its functioning (2003, p. 405). Susan W. Brenner has added what could well be deemed an important caveat to this and similar definitions. For Brenner, what is at stake in terrorism, and by extension, cyberterrorism, is the demoralization of a civilian population, which distinguishes the phenomenon of terrorism from warfare, inasmuch as the latter does not explicitly target civilians (2006, 457). She stresses that the attacks on the World Trade Center were "intended to destroy a premier symbol of capitalism and in doing so undermine the morale of US citizens and the stability of US society" (2006, 457-458).

While, both cyberwarfare and cyberterrorism can be conducted for political reasons and can result in violence against persons or property, generating fear, there appears to be a clear difference in intent. The effects of cyberwarfare on civilian populations can be deemed collateral damage, whereas cyberterrorism specifically intends to disturb and frighten civilians. Nonetheless, what is missing in several definitions circulating in the discourse of cyberterrorism, including those of Denning and Brenner, is the specification of just who the actors that perpetrate these attacks are.

Joe Wesley Moore has looked more specifically at the actors involved in cyberterrorism and draws upon international law to help specify how warfare and terrorism are distinct. He argues that International law protects "lawful combatants" who engage in combat activities" (2002, p. 27). In contrast, regarding terrorists, Moore stresses that terrorists are usually not considered to be lawful combatants, even when armed forces are deployed to fight then, Therefore, they may not enjoy "prisoner of war" status when captured and they may be deprived of the very due process of law afforded prisoners of war under the Law of Armed Conflict (Joe Wesley Moore 2002, p, 27).

One could thus assume that terrorist activities are perpetrated by sub-state actors rather than by states themselves. Nonetheless, there remains a gray area concerning those states which are sponsors of cyberterrorist acts. This problem notwithstanding, for the purposes of the present discussion, it can be assumed that cyberterrorist attacks are intentional, and in a premeditated manner perpetrated against civilian or other combatant targets by subnational groups.

In contrast to the extensive discourse on cyberterrorism in the US and other western nations, discussions in Russia are relatively sparse. Vadim R. Atnashev and Sadaf N. Yakheeva argue that the lack of an agreed-upon definition of cyberterrorism has slowed down international efforts to counter the problem. They refer to a paper delivered by R.R, Absatarov (2018, p. 173) at the Sixth International Scientific and Practical Conference in Penza, Russia, which defines cyberterrorism simply as “the use of computers as weapons or targets of politically motivated international or national groups that cause or threaten to cause damage or panic to pressure a population or government to change policy” (Vadim R, Atnashev and Sadaf N, Yakhereeva 2019, p. 38). This definition is clearly in line with some of the simpler and earlier US interpretations of the phenomenon. In a like manner, Viktoria Andreyevna Prokopeva defines cyberterrorism as “a deliberate and politically-motivated attack on information systems that endangers the life or health of people or causes the onset of such a threat” (2017, p. 12) (translation Bruce Williams). She stresses that the event perpetrated must be committed with the specific aim of violating public safety or intimidating the population. In addition to these widely accepted goals, Prokopeva adds that a possible intended outcome may well be the provocation of military forces (2017, p.12).

As mentioned earlier, Russian definitions of cyberterrorism has drawn heavily upon Western models, despite the ideological differences that inform the situation that will inform the later chapters of this thesis. On 5 December, 2016, President Vladimir Putin approved the

Doctrine of Information Security of the Russian Federation, which defines Russian national interests in the information sphere as addressing the "objectively meaningful needs of the individual society and State in ensuring their safety and security and sustainable development in the information sphere" (Ministry of Foreign Affairs of the Russian Federation, 2016). Among the points the doctrine views as fundamental for the Federation is the assurance and protection of 1) institutional freedoms and human rights in what concerns the use of information; 2) privacy in the use of information technology; 3) information support for democratic institutions and processes of interaction between the State and civil society, and 4) the application of information technologies to preserve cultural, historical, spiritual, and moral values of the multi-ethnic Russian Federation (Ministry of Foreign Affairs of the Russian Federation, 2016). In the document, only one minor point refers to cyberterrorism. Section Three of the Doctrine, entitled "Major Information Threats and the State of Information," includes as its 13th point an acknowledgement that terrorist and extremist organizations deploy information tools to influence individual, group and public consciousness, thereby fostering interethnic and social tensions; inciting ethnic or religious hatred or hostility; spreading extremist ideology, and recruiting new supporters of terrorist activity. The document stresses that such organizations actively develop destructive tools to impact critical information infrastructure (Ministry of Foreign Affairs of the Russian Federation, 2016).

Although there is not yet a universally accepted, single definition of cyberterrorism, it is essential to note that its central components are, by and large, agreed upon. There have been fewer discussions to this effect in Russia than in the West, and Russia appears not to have devoted attention to the issue of just who cyberterrorists are. Nonetheless, there is decidedly an overarching consensus on what is entailed in a cyberterrorist attack that could, if it were not for other factors, lead to greater cooperation between Russia and the West to counter possible attacks. The issues preventing cooperation appear not to entail divergent definitions of the phenomenon,

A Brief Review of Literature

The following brief review of existent literature on subjects germane to this thesis does not repeat the references woven into the above discussions of and historical perspectives on cyberterrorism. These discussions provide an insight into the state of the field and the complex search for definitions of "cyberterrorism" and related issues. Rather, it will then discuss existing research devoted to the participation of Russia and the US in existing cybersecurity initiatives and regimes.[7]

Russia and the US: Activities in cyberspace and mutual perceptions

David Bagge (1999) contrasts diverse national strategic approaches in cyberspace and analyzes Russia's cyberwarfare campaign. He details the importance of operations in cyberspace and examines why Russia's cyber activities, dubious or not, are highly successful. Bagge delves into Russian perspectives on cyber power and foregrounds specific case studies, among these the use of cyberspace in Russia's campaigns in eastern Ukraine and the Crimea. Although the discussion does not specifically address cyberterrorism, it is essential for understanding Russia's overall perception of cybercrime and large and cyberterrorism specifically.

Expanding the above discussions to an analysis of the distinction between Russia's views on the nature and use of cyberspace and those of the West, Keir Giles (2012) stresses that Russia is concerned by the uncontrolled exchange of information across its national borders, perceiving this exchange as a threat to national sovereignty. Giles examines two recent Russian public statements on cyberspace: the "Draft Convention on International Information

Security" (2011) and the "Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space." He explains that Russian authorities considered protests over the State Duma elections in 2011 to be the result of a cyber-information war against Russia. Giles examines the potential of a dialogue between Russia and the West on cyberspace.

Russia and the US—impediments to the development of a counter cyberterrorism regime

One of the primary obstacles to establishing a counter cyberterrorism regime between Russia and the US has been ideological, and bears, in part, on the relationship between establishing a regime and divergent perspectives regarding democratic processes and human rights. Tabaksky, Lior (2013 acknowledges that both open and closed societies share a common standpoint on the sociopolitical impact of information and communication technology. Specifically, both feel that the cyber realm can influence ideas, regulate behavior, and promote human rights and international security. Tabaksky advocates for Popper's scientific method to explore the influence of cyberspace on the democratic process and human rights. He hypothesizes that as ICT availability expands, political freedom should be increasingly experienced. These issues will be analyzed in more depth in Chapters IV and V.

Discussions on human rights bring to bear on debates regarding equity in access to security in developing countries. Russia's involvement in BRICS has led to criticism to this effect from Western Sources. BRICS, like the Shanghai Cooperation Organization referenced in the introduction, has been one initiative in which Russia has played a role in counter cyberterrorism. This initiative, however, has not seen complete backing from the West. Arguing that the cybersecurity issues that affect the BRICS nations also exist in many emerging and developing economies, Nir Kshetri identifies a disparity between written laws and what can be enforced in reality. Resources for such enactment are direly needed. Kshetri argues that the state of affairs in some 145 developing countries are even worse than in BRICS, since less developed countries are not subject to the same degree of pressure to enforce measures to strengthen cybersecurity. It is essential that major industrialized economies be prepared to assist and support developing nations in developing a suitable regulatory framework.

Assessing Russia's stance towards cooperation with the US on issues of cybersecurity, Julein Nocetti argues that, for Russia, the internet represents a virtual extension of the US, and its goal is to counter this phenomenon by forging new alliances. At the same time, it is seeking increased cyber diplomacy with the US. Dialogue between the two countries to this effect is difficult due to their divergent ways of looking at the internet. For the US, the issue is more technological. For Russia, it is more philosophical and political. The US appears to be primarily obsessed with guarding its technology from disruption. Russia, for its part, is asserting the maximum state power in the governance of cyberspace, and has extended the concept of the cyber realm to changing diplomatic contexts

Along similar lines, two chapters of interest have appeared in Andrey Korunov and Olga Oliker's edited volume, *A Roadmap for U.S.-Russian Relations.* These chapters deal with US and Russian stances on cybersecurity. James A. Lewis's chapter analyzes problems, from the point of view of US perceptions, that have stalled the process of US/Russian cooperation on measures to counter cyberterrorism. He explains that one of the primary problems has been that Russia has issues with the Universal Declaration of Human Rights, which the US strongly supports, and which bears upon measures to counter cyberterrorism. The US, moreover, feels that Russia deems NATO's cyber doctrine to be destabilizing and that this doctrine could sanction preemptive attacks. Given that both US and Russia have used cyberattacks for coercive purposes, the issue becomes more complex. Both nations must come together to counter cyberterrorism in a way that accommodates the political interests of both countries.

Pavel Sharikov (2017) asserts that, from a Russian perspective, the US has shifted its strategy in the fight against cyberterrorism from global frameworks to bilateral agreements. The US directly opposed a Russian proposal for an international body on cyberterrorism within the rubric of the U.N. Russia acknowledges the current strained relations it has with the US and recognizes that each has deployed cyberspace to its own agenda. In any case, an eventual accord must consider each nation's legal, political, economic, and social context. Moreover, Russia and the US must agree that the use of cyber techniques against each other destabilizes a bilateral relation and has a broader global impact.

Mohammed Riaz Shad (2018) has explored issues that are causing friction between Russia and the US regarding cyberspace, both having been accused of employing cybertechnology for espionage. According to Shad, Western sources have indicted Russia's use of cyberattacks against Estonia, Lithuania, Georgia, and Kyrgyzstan during 2007-2009 alone. They argue that, it has backed cyber-operations against Ukraine, the US, Germany, France, and the Netherlands during the Ukrainian Crisis (p. 46). Regarding the US, Shad stresses that both WikiLeaks and the Edward Snowden incident brought to light the use made by US embassies of cybertechnology in "low-level" spying against diplomats and leaders (2018, p. 47). According to Shad, Russia's use of cyberspace constitutes cyber warfare, and it has used this to collect sensitive information aimed at manipulating public opinion and undermine government authorities. Shad cites Thomas Rid, who identifies three types of cyber-attacks: sabotage, espionage, and subversion (Tomas Rid 2011, p. %), and argues that Russian attacks against Ukraine, Georgia and Estonia have fallen into all three categories (Mohammed Riaz Shad 2018, p. 47). Shad stresses that, despite the US and Russia's commitment to cybersecurity diplomacy in 1998, many events have caused it to stall. These include both Russia's offering political asylum to Snowden and refusal to extradite him, as well as its alleged interference in the 2016 US elections (Shad 2018, pp. 49-51). Shad discusses, as well, differences between Russian and US conceptions of cyber ethics and the overall domains of cybercrime and cybersecurity. These will be discussed at length in Chapters IV and V of this thesis.

Gaps in Existing Literature

Despite an ongoing search for an exact definition of cyberterrorism, there is extensive literature on the phenomenon, although a good deal of it falls under the general rubric of cybercrime. There have, moreover, been numerous studies that have ventured a contrast between cyberwarfare and cyberterrorism, although, once again, definitions are still in a state of flux. Existent literature on the topic is heavily weighted towards a US/EU perspective. Analyses on Russia's stance on the issue are more limited in comparison. There have been a number of studies on the creation of international regimes to counter cyberterrorism, and some of these efforts will be discussed in Chapter III of this thesis. There have, moreover, been pieces that allude to potential cooperation between Russia and the US to confront the potential problem. To date, Mohammed Riaz Shad has offered one of the most complete studies of these problems, exploring both historical issues that have posed problems to the development of a cyber regime between Russia and the US, and significant distinctions between the two countries general approaches to cyberspace. To date, the specific question of the development of a US/Russia regime specifically to fight cyberterrorism has not been explored Many of the problems identified by Shad will doubtless come to play in this issue, however, what is missing in existing scholarship is a systematic and multi-pronged analysis of why efforts proposed or partially undertaken by the two superpowers to this effect have failed.

CHAPTER II

THEORETICAL PERSPECTIVE: CONSTRUCTIVISM AND STRATEGIC CULTURE

A realist approach cannot completely explain the puzzle of the failure of Russia and the US to establish a counter cyberterrorism regime. Given that both states have undergone considerable ravage from terrorism—one need only think of the 1993 and 2001 attacks on the World Trade Center, the 2002 hostage crisis in a Moscow theatre, the 2004 and 2010 bombings of the Moscow metro, and the 2013 bombing in Volgograd, to name but a few--, and both could be victims of current threats, either internationally or domestically orchestrated, the two superpowers share vulnerability. When one adds a cyber dimension to these threats, the advantage of a competent security regime becomes immediately evident. A rational actor would doubtless weigh the benefits of increased security against any advantage such cooperation might afford the competitor. After all, as will be discussed in Chapter III, the US has successfully involved itself with such initiatives in Europe and the Americas, and Russia has participated in cyber cooperation with BRICS and with the Shanghai group. Moreover, both Russia and the US have articulated their willingness to cooperate with each other to this effect. However, as will be explored in Chapter IV, such promises have never come to fruition. There must be another paradigm that can be used, if not to predict behavior, but at least to explain the reticence on both sides to develop a counter cyberterrorism regime.

For a realist, whose primary focus is the sovereign state as an actor in the international system, other institutions are deemed to have considerably less influence. Hence, individuals, multinational corporations, NGOs, and even trans-state initiatives are downplayed, favoring the interests of the state, and the balance of power among states. However, the case of attempts to build a counter cyberterrorism regime between Russia and the US is considerably more complex and involve far more than the two nation states as actors.

Social Constructivism as a Critical Approach

Social constructivism as an overarching philosophy presents an alternative to realism. The concept had been circulating in other branches of the social sciences for a good number of years,[8] and made its way into the field of international relations over the course of the 1980s. In an extended analysis of transformations in the field of international theory, Richard Price and Christian Reus-Smit posit that three factors which worked in tandem to promote the adoption of constructivism as a viable discourse in international relations: 1) the interface between neoliberalism and new discourses in critical theory, 2) the demise of the Cold War, which could not be explained by rationalist theory, and 3) the emergence of young international relations scholars, who had been entrenched in critical theory (1998). Of primary concern to social constructivists in international relations has been "the examination of nonmaterial factors such as norms, ideas, knowledge, and culture" […] (Hoyoon Jung 2019, p.2). Martha Finnemore and Kathryn Sikkink stress that constructivism in social analysis deals with "the role of human consciousness in social life" (2001, p. 391). They argue that ideational factors define human interaction as opposed to material interests. Moreover, the most significant ideational factors are widely shared among members of a group. Expanding this notion to international relations, they argue that the prime importance of constructivism lies in its theoretical arguments instead of empirical research methodology (2001, p. 391). Finnemore and Sikkink foreground the importance of the interpenetration between international affairs and domestic politics and the connection between transnational social movements and ones which operate on a domestic level. They explore how the understanding of domestic political and ideational processes inform questions of when and why international cultures and norms impact on individual domestic settings. (2001, p. 411). In the case of the failure of Russia and the US to be successful in the formation of a counter cyberterrorism regime, both domestic politics and the formation of ideas may well play a significant role in the reticence of both states to work harmoniously towards such a goal.

Drawing the discussion from the broader debates surrounding international relations to the specific domain of security studies, Yu-tai-Tsai identifies a number of key tenets of constructivism that interface with debates in the field. These include: 1) the nature of social structures, which is composed of shared knowledge, practices, and material resources; 2) the belief that norms, customs, culture, and learning can change the interests a behavior of a nation's citizens; 3) the assertion that it is the interaction between countries that generates identity and interests; 4) the concept that the international community and the structure of the political system are interdependent upon each other, and this interdependency determines the direction the international system will take, and 5) an emphasis on the concepts of norms, identity, and culture (2009, pp. 21-22).

Peter Katzenstein (1996), applies such concepts to security studies, stressing, along similar lines the importance of *norms*, which describe "the proper behavior of actors with a given identity" (1996, p. 5) and that *of identity*, "which is a shorthand label for various constructions of nation- and statehood" (1996, p. 6). His arguments strongly parallel those of Benedict Anderson on the nature of nationalism. For Anderson, one of the prime components of nation building is the notion that a nation is fabricated and defined by shared experiences. Anderson posits:

> [A state is] an imagined political community—and imagined as both inherently limited and sovereign [...]It is *imagined* because the members of even the smallest nation will never know most of their fellow members, meet them, or even hear of them, yet in the

> minds of each lives the image of their communion […] The nation is imagined as *limited* because even the largest of them, encompassing perhaps a billion living human beings, has finite, if elastic boundaries, beyond which lie other nations […] Finally, it is imagined as a *community* because, regardless of the actual inequality and exploitation that may occur in each, the nation is always conceived as a deep horizonal comradeship (1983, pp. 6-7).

Although Anderson's notion of imagined communities was elaborated to address the origins of nationalism, it, nonetheless, has implications for international relations, and specifically, security studies, in that it posits the notion of a state that is defined not by self-interest and its need for a balance of power, but instead by more complex and intangible factors. By implication, the "imagined community" of one state may well be considerably distinct from another.

Along similar lines, Jef Huysmans explores the influence of security language on domestic processes. He notes a tendency in political and academic discourse to relate such issues as terrorism, drugs, immigration, and asylum to the realm of security. In other words, issues of cultural/ethnic identity and public order, both of which have traditionally been regarded as domestic issues, have penetrated the realm of international security (Jef Huysmans 2002, p. 41). His analysis reexamines the work of Ole Weaver et al, which question the consequences of the integration of identity issues into the security arena upon the reconsideration of a European order in the post-Cold-War era. At stake is the legitimization of non-state security policy and the de-legitimization of the state that "should" have the role of protector of society. This project, according to Weaver et al, becomes dangerously close to fascism inasmuch as such an approach could lead to xenophobia and nationalism against foreigners (Ole Weaver et al 1993, pp. 188-189). Nonetheless, Huysmans argues quite the opposite, that the presence of security language in other aspects of society may well lead to a stronger and more intense prioritization of issues of human rights or efforts to combat the conservative bias of security language. In this respect, security is defined as a positive process that considers the liberation from oppression as a positive goal to be reached (Jef Huysmans 2002, p.59) Finnemore and Sikkink's analysis as well as that of Huysmans focus on the impact of international processes on domestic ones. If one accepts their agenda, then a reversal of the process may well prove a valid approach. International dynamics may well be shaped in part by domestic ones, the domestic and international never being completely separate. These debates, which bear upon culture and national identity, are likely to reveal insights into substantial differences between Russian and US ideologies that could well hamper regime formation.

During the Cold War, the West attempted to understand the political strategy and behavior of the Soviet Union through Soviet ideology, with specific attention being devoted to the impact of Leninism and Stalinism on current processes. Frank L. Jones, Jr. (2012, p. 287) traces the origin of this approach to the work of Nathan Leites, who sought to explore the influence of Soviet ideology on policy calculations, both foreign and military (Nathan Leites 1951, pp. xxi-xxiii). For Leites, Leninist and Stalinist texts provided the best possible means for understanding the rules of Soviet strategy. Jones follows his chronology of such cultural analysis by foregrounding the work of Alexander L. George, who discussed the notion of general belief systems, which influence the interpretation of leaders of the stream of political events and understanding of specific situations and bring to bear upon their decision making (Alexander L. George 1967, p. v). The notion of operational code constituted a theoretical mediation that led, a decade later, to the development of the notion of strategic culture. In 1977, Jack L. Snyder employed this concept, not to predict Soviet behavior, but instead to understand "the intellectual, institutional, and strategic cultural determinants" that would affect Soviet reactions to limited nuclear on the part of the US (Jack L. Snyder 1977, p. iii). Snyder's study was a pivotal moment in the development of the concept of strategic culture among academics.

Given the limitations of realist approaches for shedding light on the behavior of Russia and the US in what concerns the formation of a counter cyberterrorism regime, the general precepts of social constructivism may well prove to offer significant insights into the ideational underpinnings that define the behavior of the superpowers. Further insight is likely to be gained from the use of a related sub-concept, that of strategic culture.

The potential of a strategic cultural approach

Rashed Uz-Zaman stresses that one of the main difficulties in defining "strategic culture" lies in the problem of defining "culture" itself (2009, p. 69). To answer this question, he draws upon the work of Raymond Williams, who identifies three general categories that together constitute the nature of culture, the "ideal," the "documentary," and the "social." The ideal category seeks out ideas that are constitutive to values that are integral to a timeless order. The documentary level frames culture through the lens of the recorded body of human thought and experience. Finally, the social views culture as a "description of a particular way of life that finds meaning in, among other things, institutions and ordinary behavior" (Uz-Zaman, 2009,p. 70). For Williams, each of these categories is an essential component of culture, and any definition lacking even one of them is deficient.

Over the last four decades, proponents of this critical approach have been divided into four distinct generations, each with a distinct perspective on both the relationship of strategic culture to other analytical approaches (such as the realist school) and what constitutes suitable academic rigor in the approach. The following discussion will not examine the precepts of the four generations nor the tense debates among the proponents of each. Instead, it will foreground the overall essentials of strategic culture and suggest how such theoretical positions can be modified to explore the failure of Russia and the US in regime formation. Drawing his discussion from broader discourses of culture into the realm of strategic culture, Uz-Zaman clarifies that it was during the Vietnam War and the US-Soviet Union nuclear confrontation of the Cold War that made it clear "a coherent concept was needed to understand why countries thought about violence and waged war in different ways" (2009, p. 71). Uz-Zaman explores Colin S. Gray's desire to probe beyond the rational actor approach and look at distinctions among local contexts. He further explores the work of Adda B. Bozeman who criticized claims that international violence resulted primarily from the underdeveloped status of many newly-formed independent states and argued that such in such claims, "no allowance was made for the possibility that war-related phenomena might be, perhaps even predominantly, aspects of locally prevalent values, images, traditions, and mental constructions" (Adda B. Bozeman 1976, p, 77).

In this respect, Bozeman's work constitutes an integral part of those critics who challenge the ahistorical and non-cultural framework of neorealism to analyze strategic decisions. Alastair Iain Johnston, in a manner not unlike Bozeman, stresses that neorealism discredits an actor's accumulated past and focuses instead on a forward-thinking speculation regarding utility. Neorealism assumes that states are "undifferentiated units that seek to optimize their power, which can be measured by "capabilities and resources" (1995, p. 35). "Strategic choices will be optimizing ones, constrained only, or largely by variables such as geography, capability, threat, and a tendency of states to refrain from behaviors which threaten their immediate survival" (1995a, p. 35). Johnston explains that the lens of Strategic Culture argues that the elites of given strategic culture will make "different choices when placed in similar situations" (1995a, p. 35).

Johnson identifies three levels on which early proponents of strategic culture based their analyses: "a macro-environmental level consisting of geography, ethnocultural characteristics and history; a societal level consisting of social, economic, and political structures of society; and a micro level consisting of military institutions and characteristics of civil-military relations" (Alastair Iain Johnston 1995a, p. 36). Nonetheless, Johnson criticizes the notion of a strategic culture which comprised technology, geography, organizational culture and traditions, historical strategic practices, political culture, national character, and political psychology all playing relevant roles. He further cautions against highly simplistic conclusions, such as the belief that "there was one American culture, distinct from one Soviet strategic culture, which made the United States incapable of fighting and winning a nuclear war" (1995a, p. 36). He also deems it problematic to believe that a society's strategic culture was homogeneous across time.

A good deal of the early work in strategic culture was devoted to the Soviet Union and attempted to explain Soviet behavior to western strategists. However, the agenda of the proponents of strategic culture expanded and was soon used to study US behavior. In 1981, Colin S. Gray examined the "American style in strategy." Gray bases his study in part on earlier analyses of Soviet strategic culture, arguing that, in the Soviet Union, "individuals are socialized into a distinctive Soviet mode of strategic thinking" (Colin S. Gray 1981, p. 21). For Gray, this has placed Soviet strategists on a cultural level as opposed to merely upon a policy level (1981, pp. 21-22). Scholarly speculations regarding Soviet strategic culture led Gray to hypothesize that there is:

> […] a discernible American strategic "culture": that culture referring to modes of thought and action with respect to force, desires from perception of the national historical experience, aspiration for self-characterization (e.g., as an American, what am I? how should I feel, think, and behave (1981, p. 22).

These thoughts combine with other distinctively American experiences, which include, but are not limited to, geography, political philosophy, civic culture, and way of life (1981. p. 22).

Consequently, there must be a “distinctively American way in strategic matters” (1981, p. 22). Gray deems that US strategic culture oscillates between extremes, both extremes being “quintessentially American” (1981, p. 44). Examining US behavior towards the Soviet Union in the 1970s, Gray posits that the US believed that the two superpowers had a tolerably congruent perspective on the optimal status quo and that reason dictated that the physical protection of Americans was predicated upon pre- or intra-war deterrent effects. While policy maker sought for flexibility, US strategic force were postured for an ever-so-short war (1981, p. 45). Gray sums up the contradictory nature of US security culture by stressing that Americans are unlikely to behave in a manner contradictory to “what they are” (1981, p. 46). Gray concludes his argument by arguing that in the 1980s, the combination of Soviet and US (strategic) cultures “have produced, in competition, a dangerous shortfall in sustained defense efforts on the American side” (1981, p. 47).

Uz-Zaman further describes the use of strategic culture to foreground notable disjunctions between what leaders believe their rhetoric means and the deeper motivations that underlie what they in all actuality do. He discusses the work of Bradley S. Klein, who explores how states use internationally deployed forces to project leadership within their internal borders. Since states often evince a dichotomy between rhetoric and operational policies, Klein feels that the primary duty of strategic culture is to “historicize what has lain implicit in realist theories of hegemony” (Bradely S. Klein 1988, p. 136). Uz-Zaman examines how strategic culture draws heavily upon cultural interpretations and is closely aligned with issues in domestic structure and organizational structure. In this respect, it is decisively influenced by constructivism (Uz-Zaman 2009, p. 78). He refers to the work of Theo Farrell, who considers contemporary work in strategic culture a merger of culturalism, which was derived from comparative politics, sociology, and anthropology, and constructivism as employed in security studies. This synthesis of approaches facilitated viewing “actors and structures much differently than the rationalist approaches to international relations […] locating actors in a social structure that both constitutes those actors and is constituted by their interactions" (Theo Farrell 2002, p. 50). Scholars who work along these lines examine such issues as military culture, political military cultural, and organizational cultures, and all are firmly united in debunking realist theories (Alastair Johnston 1995b, p. 18-19). In a similar manner, Michael Desch notes a predominance of studies focusing on organization, political, strategic, and global culture.

Other proponents of strategic culture focus their analyses on the role of elites. Tamir Libel recoups the early work of Jack L. Snyder, who asserted that strategic culture consists of "a set of semipermanent elite beliefs, attitudes, and behavior patterns socialized into a distinctive mode of thought" (Jack L. Snyder 1977, p. 66). According to Libel, the elites express specific strategic cultures in what concerns military activity which are socialized into a given mode of strategic thinking (Tamir Libel 2016, p. 140). Libel stresses that by employing the term "semipermanent," Snyder opened critical discourse up to the possibility of change in strategic culture. He reaffirms Johnston's claim that while diverse cultures could exist within a strategic culture, one would have to be dominant and hold invested interests which favor the status quo and thereby shape the ideational stance of the national strategic elites (Tamir Libel 2016, p. 140). Such observations suggest that Russia and the US's elite cultures and dominant belief systems significantly impact on their strategy.

Strategic culture does not simply apply to military strategy and should not be conflated with it. Instead, it is a concept employed to explain behavior that is, at least in part, independent from material power potential. This thesis argues that strategic culture has explanatory potential for the case of Russia and the US's failure to form a counter cyberterrorism regime. This potential will be tested in Chapter V, where the successes and failures of both superpowers in cooperation and regime formation will be assessed.

CHAPTER III

RUSSIA AND THE US IN INTERNATIONAL CYBER REGIMES AND COOPERATION EFFORTS

Inasmuch as the aforementioned Dogrul, Aslan, and Celik are affiliated with Turkey's Air War College in Istanbul, they advocate in part for a military strategy to counter the prospect of cyberterrorism. Yet, like many of their international colleagues, they also support international conventions and regimes to address the issue. The authors stress that it is essential to have an accepted definition of both terrorism and cyberterrorism and to determine those internet activities that constitute cyberterrorism. As they stress, "Speaking the same language or creating a common technical language could be a commencing point" (2011, p. 41). Secondly, national and international legal arrangements should be realized, and harmony established between national laws and international legislation. Thirdly, bilateral and multilateral accords on cybersecurity in general should be established. Subsequently, an intelligence pool should be developed in order to collect and share intelligence among nations. This information should focus not only on terrorist websites, but also on the collection of evidence for any eventual cyberattacks. Dogul, Aslan, and Celik further advocate for the creation of response teams and the development of response training programs. International counter-cyberattacks should be planned and executed in order to aid with the sharing among nations of proficiency and expertise. Responses to attacks should be based on mutually accepted rules of execution. And finally, an after-the-fact analysis should be made with the purpose of identifying and improving improve weak elements of the system in place (2011, p. 41).

A number of international accords are in place which deal with potential cyberterrorist acts. Most of these, however, fall under the broader rubric of the establishment of cybersecurity regimes. International accords normally come into place once an individual nation already has a cybersecurity infrastructure in place. To address this need, the International Telecommunication Union (ITU) held a workshop in Doha, Qatar in February 2008, which was intended to help Arab nations develop a framework for cybersecurity. One of the main premises of the workshop was that each individual country must join and support international efforts to improve cybersecurity. The workshop was intended to introduce countries in the Arab region to the actions and approaches, *lire* best practices that have proven successful in other regions. Although the scope of the workshop focused specifically on the Middle East and North Africa, its broader implications can be applied to virtually any case. The intended goals of the workshop included, but were not limited to 1) assisting nations with the development of national strategies for cybersecurity; 2) aiding in the establishment of national government-industry collaborations; 3) fostering to deterrence of cybercrime; 4) fomenting the creation of national incident management capabilities, and 5) promoting national cultures of cybersecurity (International Telecommunication Union 2008, p. 16).[9]

Each of the two superpowers has been involved in more than one regime to foster cybersecurity, although they have failed to develop a similar regime together. The mere fact that they become a part of cybersecurity regimes, or of agreements in which cybersecurity plays an important role, indicate two important positive directions. Firstly, such agreements strongly indicate that the formation of cybersecurity regimes is indeed possible. Secondly, they show that both Russia and the US have demonstrated favorable dispositions to participate in these regimes.

Russia’s Participation in Cybersecurity Regimes and Accords

Both Russia and the US, hves been individually involved in numerous initiatives which have involved, at least tangentially if not significantly, cybersecurity. While the foci of these initiatives may well be distinct from the notion of counter cyberterrorism, the participation of the two superpowers in them attests to a willingness on both parts to participate in closely-related international cooperative initiatives. In light of their primary objectives, these diverse cooperative efforts have had very divergent impacts on countering cyberterrorism. Nonetheless, in virtually all cases, activities could easily be expanded to embrace these efforts. It is essential to note that, at least in the case of Russia, one of the country's cooperative agreements, participation in the Shanghai Cooperation Organization, predated a number of terrorist attacks and cyber incidents that characterized the first decade of the new millennium. These attacks brought home the need for Russia to address issues of terrorism. Russia, as a superpower, is moreover very vulnerable to cyberattacks. A cyberterrorist act against Russia, whether coupled with a physical attack or not, could inflict unprecedented devastation. It seems to be in Russia's advantage to participate in a cybersecurity regime.

Additionally, as part of BRICS (an association of five major emerging economies comprised of Brazil, Russia, India, China, South Africa), Russia is now participating in a new cybersecurity regime. A 2019 meeting of the BRICS communications managers held in Brasilia established CyberBRICS, a security alliance which recognized the need for strategies and well-informed policies to create synergy among BRICS members to counter cybercrime, in full acknowledgement that BRICS countries are both the main targets of cyber-attacks and the site of origins which most cyberattacks occur (Luca Belli 2019). CyberBRICS has as its stated goals "[…] to map existing regulations, to identify best practices and develop policy suggestions in the areas of cybersecurity governance (including personal data regulation), Internet access policy and strategies for the digitalization of public administration in the BRICS" (CyberBRICS 2021). The project is jointly hosted by the Fundação Getúlio Vargas Law School (Rio de Janeiro); the Higher School of Economics (Moscow); the Centre for Internet and Society (New Delhi); Fudan University (Shanghai), and the University of Cape

Town. The CyberBRICS team is composed of international academics from both BRICS and other countries. Russia's primary members on the team are Andrey A. Shicherbovich of the Department of Constitutional and Municipal Law of the Higher School of Economics and Anya Orlova, who holds an M.A. in psychology and sociology and currently works in digital activism and advocacy (CyberBRICS 2021).

The sole reference to terrorism made on the website of CyberBRICS is included in a discussion of the processing of personal data by the countries of the bloc. Although it does not specifically refer to cyberterrorism, it is mentioned together with cybercrime. The reference is relatively vague, yet it is made clear that Russia legislation permits the processing of personal data for reasons of defense, security, countering terrorism, transport security, countering corruption, criminal investigation, insurance legislation, executive legislation, state social assistance, and labor and pension legislation (CyberBRICS 2021). A good deal CyberBRICS' work on cybersecurity tends to be oriented towards a comparative analysis of cybersecurity policies in individual country members rather than on the development of cooperation (Luca Belli 2021). Although CyberBRICS cannot be deemed a regime to counter cyberterrorism or even cyberwarfare, the mere fact that Russia is willing to discuss openly with other member states its policies on the use of personal data reveals.

More closely related to the issue at hand than Russia's participation in CyberBRICS is its work with the Shanghai Cooperation Organization. I, 1995, China, Russia, Tajikistan, Kyrgyzstan, and Kazakhstan met to develop a cooperative regime. Known as the "Shanghai Five," the group drafted a joint statement Tajikistan in July 2000 to strengthen cooperation; fight illegal activities; foster the respect for national sovereignty; promote respect for the 1972 Anti-Ballistic Missile treaty, and foment regional security ("'Shanghai Five' Nations Sign Joint Statement" 2000). By 2001, the group had made considerable progress in building its economic, military, and diplomatic relations (Gil Gates, 2001), and it was reconceived as the

Shanghai Cooperation Organization. The Group consisted of the original Shanghai Five together with Uzbekistan. Today, present-day members include Russia, China, India, Pakistan, Tajikistan, Kyrgyzstan, and Kazakhstan.[10] The Organization has as its four main areas of concern cooperation on 1) security; 2) military activities, 3) economic development, and 4) cultural exchange. Counter cyberterrorism, although not specifically mentioned as an area of concern, falls under the broader rubric of security.

Atnushev. and Yakheeva (2019), all the while emphasizing that Russia's national security strategy does not contain the term "cyberterrorism," have provided a concise assessment of Russia's involvement in the Shanghai Cooperation Organization in what concerns the challenges of cyberspace. In January 2015, Russia, together with other members of the Organization, submitted to the UN General Assembly what it determined was the first international document on the standards of cyber conduct in the international environment. As Atnushev and Yakheeva clarify, the objectives of the document were to 1) define the rights and obligations of states in cyberspace, 2) encourage constructive and responsible behavior by the State, and 3) foster cooperation against the threats and challenges in cyberspace (2019, p. 40). According to Atnushev and Yalheeva, the document submitted by the Shanghai Cooperation Organization led to the adoption by the UN General Assembly of a resolution on developments in the field of information and telecommunications in the context of international security. The resolution was supported by 119 states, with 49 countries voting against, and 14 abstaining. The authors stress that work is underway on a UN convention on international information security (2019, p. 40). As will be discussed in Chapter IV, it is significant to note that the US did not support the resolution, but rather it felt that the Shanghai Cooperation Organization had undermined other international initiatives by submitting the resolution.

US Participation in Cybersecurity Regimes and Accords

The US, for its part, is a signatory, along with 55 other countries, of the Budapest Convention on Cybercrime, which, despite its broader scope, also deals with the potential of cyberterrorism. The Budapest Convention was drafted and made open to state signatures on 23 November 2001. It constituted the first international treaty on crime committed by means of the internet or through the use of other computer networks. Its main foci were copyright violations, computer fraud and infringements upon national security. It further defined protocols for the efforts involving the search of computer networks and interception activities (Council of Europe Treaty Office 2021). The US was one of the first signatories of the Convention, having signed on the first day the document was made available. In its Preamble, the Convention articulates, together with its stated goal of facilitating the detection, investigation, and prosecution of cybercrime at both domestic and international levels and providing a protocol for international cooperation, the importance of respecting the European Court of Human Rights' 1950 Convention for the Protection of Human Rights and the United Nations' 1966 Covenant on Civil and Political Rights (Council of Europe 2001, p. 2).

In 2009, Michael N. Schmitt, chairman of the International Department of the US Naval War College, became the leader of a team of international experts in drafting what became known as the *Tallinn Manual on the International Law Applicable to Cyber Warfare*. The participants in the project were professionals from the Netherlands, Sweden, Switzerland, Belgium, Germany, the UK, Australia, Canada, and the US. The US participation in the drafting of the *Manual* involved four academics. Although the *Tallinn Manual* has come to be conflated with NATO, and credit is often given to NATO for its preparation, the individuals involved in the development and drafting of the work referred to themselves as the International Group of Experts. The front page of the *Manual* credits the authorship as the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of

Excellence. Hence, although the *Manual* was not actually prepared by NATO, it was produced under its auspices. The *Manual* credits as well three organizations that provided observers to the process of drafting the work: the US Cyber Command, NATO's Allied Command Transformation, and the International Committee of the Red Cross. The observers could freely take part in discussions, but their consent was not necessary in decision making. The role of the representative of the US Cyber Command is described as "[offering] the perspective of a relevant operationally mature entity" (Michael N. Schmitt 2013, p 10). Clearly, the US assumed a leadership role in the preparation of the work, and the *Manual* is one of the salient examples of US cooperation to combat cybercrime and cyberwarfare. The "Introduction" to the *Manual* credits the US Naval War College for having held the first major legal conference on the subject in 1999. This initiative, as explained, was overshadowed by the 9/11 terrorist attacks, yet began to draw international attention following hacktivist attacks against Estonia in 2007 and Georgia in 2008, coupled with targeting on Iranian nuclear facilities with the Stuxnet Worm in 2010 (Schmitt 2013, pp. 1-3).[11] The stated scope of the *Tallinn Manual* is to encompass both "the international law governing the resort to force by States as an instrument of their national policy" and "the international law regarding the conduct of armed conflict" (Michael N. Schmitt 2013, p. 4). The *Manual*, moreover, does not affect such other international laws as those referring to human rights or telecommunications (2013, p. 4). The *Manual* intentionally does not deal with such problems as cyber espionage, the theft of intellectual property, and other related cybercrimes since these are not related to the use of force. The notion of terrorism, moreover, is simply not addressed by the *Manual*, Nonetheless, the participation of the US in the development of two editions of the *Tallinn Manual* provides strong evidence for the nation's commitment to participate in international efforts in the domain of cybersecurity.

The US further cooperates in efforts against cyberattacks with NATO. Recently, the Montenegrin Minister of Defense, Predrag Bošković, asserted that the US has aided in the protection of democracy in the Western Balkans "from those who would keep this part of Europe in conflicts, setbacks and economic decline" (US Embassy in Georgia, 2020). Further, the US has offered assistance to Ukraine and North Macedonia in the defense of their cyber networks. In all of these cases, the alleged perpetrator of cyberattacks has been Russia.

Regarding the western hemisphere, the US has been involved in the development of cyber initiatives in Latin America and the Caribbean. In January 2020, it provided 10 million dollars under the Digital Connectivity and Cybersecurity Partnership (DCCP) for ventures that foment private sector investment in energy and infrastructure (US Department of State, 2020). The work to this effect is championed by the Growth in the Americas initiative. Growth in the Americas/América Crece identifies itself as a "whole of government" effort, involving the Departments of State, Treasury, Commerce, and Energy in tandem with the United States Trade and Development Agency (USTDA) and the Overseas Private Investment Corporation (OPIC). While the emphasis of Growth in the Americas/América Crece is on economic develop, security issues are not ignored. A US Department of State fact sheet regarding the initiative outlines its cybersecurity components. It explains that the US, under the DCCP, is offering its neighbors with training in cybersecurity best practices. These trainings are provided by the National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA). The State Department, moreover, supports two International Computer Hacking and Intellectual Property Advisors (ICHIPS) base in Panama City and São Paulo. These advisors are charged with strengthening international cooperation and delivering law enforcement training to combat cybercrime. The State Department further overseas cybercrime courses in the International Law Enforcement Academy, a school it supports. Regarding cyberterrorism, the US works closely with the Organization of American

States (OAS) International Committee against Terrorism, and has provided experts to help build policy and technical capacity in Latin America and the Caribbean, and to assist in the development of national cyber strategies, including the implementation of cyber confidence-building measures (US Department of State 2020).

Regarding the Latin American countries covered by the Monroe Doctrine, cybersecurity expert Mary Ann Davidson, in a 10 March 2009 testimony before the US's Homeland Security Subcommittee on Emerging Threats, Cybersecurity and Science and Technology, proposed a Cyber Monroe Doctrine, which "[…] would have the same primary view as the original Monroe Doctrine—a signal to others of our national interests and a readiness to action in defense of those interests" (Mary Ann Davidson 2009). Davidson specifies how such a doctrine must be interpreted, arguing that any consideration of the US's cyber interests must be evaluated within the broader perspective of national freedoms and security concerns. She clarifies that the defacement of a government website is quite different from a weapon of mass destruction (WMD on a major city. Essentially, all cyber risks are not created equal and do not warrant an equal response (Mary Ann Davidson 2009).

Although US efforts both regionally and with its western allies at large fall short of constituting cyber regimes, they, nonetheless provide evidence for extensive cooperation on behalf of the superpower in strengthening international cybersecurity. The cooperative efforts in which the US has engaged in Latin America, the Caribbean, and Western Europe demonstrate that the US clearly perceives itself to be a leader in this regard.

Evidence of Prior and Existing Cooperative Initiatives between Russia (the Soviet Union) and the US

Despite the failure of Russia and the US to form a counter cyberterrorism regime, it is essential to note that the two superpowers, adversaries during the Cold War and arguably adversaries until today, have successfully cooperated in other types of accords. Such accords, surprising as they may have been at times, have occurred both during the Cold War period and over the course of the last thirty years. The bonds of friendship between Stalin and Roosevelt were marred by the overall distrust on the part of the American people of the communist system. Moreover, in light of Stalin's purges, the US perceived that the Soviet Union was being run by a totalitarian dictator, equaled only by Albania's Enver Hoxha. Competition between the two foes was fierce when the Soviet Union took a clear lead in the space race with the 1957 launch of Sputnik. Doubtless, the height of the Cold War was marked by the Cuban Missile Crisis of October 1962. Distrust between the two countries was at an all-time high. The tensions were not reduced when it was learned the following year that Lee Harvey Oswald, who fired the gun that killed President Kennedy, was an American who had defected to the Soviet Union. In the prevailing climate of mutual suspicion between the wo superpowers, paranoia was prevalent. During the Missile Crisis, US school children practiced sheltering under their desks in the event of an impending bond. In the years that followed, home fallout shelters became the rage in the US, while Muscovites were somewhat comforted knowing that line three of the Moscow Metro had been constructed particularly deep so as to protect the population in the event of a nuclear attack.

Following the death of Stalin, cultural and academic exchanges between the US and the Soviet Union were ongoing. In 1956, Soviet pianist Emil Gilels and violinist David Oistrach toured the US in concerts organized by American impressarios. In a like manner US violinist Isaac Stern, tenor Jan Pierce, and the Boston Symphony Orchestra performed in Russia.[12] In 1959, exhibitions were held in New York and Moscow to reveal to Americans how Soviets live and vice-versa. Following the Cuban Missile Crisis, a monumental cross-cultural project was undertaken. This led to a regular flow in the exchange of cultural products between the superpowers. Exchanges of “specialists” also occurred in the mid-1950s and were ongoing thereafter. These included reciprocal visits by medical specialists religious leaders, and Red Cross delegations (Helen B. Shaffer, 2021). In 1958, the Soviet Union and the US agreed to extensive exchanges in industry, agriculture, public health, education, government, civic affairs, youth and student activities, motion pictures, sports, and other fields (Helen B. Shaffer, 2021. In 1963, acclaimed New York City-based television producer Lucy Jarvis was permitted to film inside the Kremlin, and her 1963 documentary, *The Kremlin*, which was made for NBC television, gave American viewers a rare look inside the forbidden land. Cultural products have traveled back and forth since then. In 1980, Soviet director Vladimir Menshov’s film *Moscow Does Not Believe in Tears* (*Moskva slezam nye vyerit*) (1979), which focused on urban life in the Soviet Union of the 1950s, attained cult status in the US. President Ronald Reagan viewed the film numerous times to prepare for his first meeting with Mikhail Gorbachev (Leslie H. Gelb, 1985, Soviet Art/USSR Culture, n.d.).

Joint efforts between the Soviet Union and the US in the realm of security developed considerably more slowly than cooperation in cultural and academic domains. Nonetheless, in the months following the Cuban Missile Crisis, a significant security effort was undertaken. A telephone hotline was installed between Moscow and Washington, which was designed to avert another similar crisis or worse. This was arguably the first cooperation effort made between the two enemies in the domain of security. Less than a decade later, the Soviet Union and the US negotiated the Anti-Ballistic Missile Treaty, which remained in effect from 1972 until 2002, when US President George W. Bush withdrew from the treaty because of the need to develop defenses against possible terrorist or “rogue-state” missile attacks (Arms Control Association, 2020). The Treaty consisted of a successful agreement between the Soviet Union and the US in which both parties agreed that by limiting defense systems, the two superpowers would reduce the need for offensive weapons.

In 1987, the Intermediate-Range Nuclear Forces (INF) Treaty constituted the first time in which the Soviet Union and the US agreed to reduce their nuclear arsenals, eliminate an entire category of nuclear weapons, and allow onsite inspections for verifications. The Treaty led to the destruction of some 2,692 short-, medium-, and intermediate-range missiles by the agreed-upon deadline of 1 June 1991 (Arms Control Association, 2019). This agreement, coupled with the ABM Treaty, failed to solve completely security concerns between the Soviet Union and the US. Nonetheless, they constituted a significant moment in cooperation between the two superpowers in the security realm. As Joseph S. Nye has argued, although the Soviet Union and the US failed to develop an overarching security regime, a number of strides were made in sub-categories of security.

Along similar lines, in 1993, an agreement between the US and Russia involving highly-enriched uranium (HEU), known as the HEU Agreement was signed whereby Russia would down-blend 500 tons of HEU, enough to build 20,000 nuclear warheads, over a twenty year period. The resulting low-enriched uranium (LEU) would be sold to the US to use as fuel in nuclear reactors. The Program the Agreement envisioned was dubbed "Megatons to Megawatts." The Program was considered by both parties to be a mutually-beneficial business deal. The Proposal was especially attractive to Russia in that the down-blending would take place in Russia rather than in the US, thereby employing as many people as possible and using numerous facilities from Russia's nuclear sector (Alexander Pavlov and Vladimir Rybachenkov. 2013). By the late 1990s, the Agreement had drawn sharp criticism in Russia due to the low price it was receiving from the sale and the threat to Russian national security through the reduction in its strategic HEU stockpiles. As Alexander Pavlov and Vladimir

Rybaschenkov stress, Russia could possibly have tried to find a better buyer for the uranium, such as Saddam Hussein. Nonetheless, as per the nuclear Nonproliferation Treaty, Russia may not "assist, encourage, or induce any non-nuclear weapons State to manufacture or otherwise acquire nuclear weapons or other nuclear explosive devices, or control over such weapons or explosive devices" (Alexander Pavlov and Vladimir Rybaschenkov, 2013). Pavlov and Rybaschenko further stress:

> The HEU-LEU deal can provide useful lessons in that regard. It proves that countries' differences, no matter how great, can be overcome if political interest is accompanied by economic benefit. Policymakers need to look for projects that combine those features. Finding such projects and implementing the experience gained in the HEU-LEU deal becomes a more urgent task every day (2013).

On 5 February 2011, the Treaty between Russia and the US on Measures for the Further Reduction and Limitation of Strategic Offensive Arms, more commonly known as the New START Treaty, went into effect. The Treaty gave both countries seven years in which to meet specified limits on strategic offensive arms. The limitations prescribed by the Treaty, moreover, were verifiable. As of 5 February 2018, both countries had met the conditions of the New START Treaty and, according to the US Department of State, have stayed at the specified limits since that time (US Department of State 2021). Eighteen onsite inspections are permitted each year by Russian and US teams. These encompass inspections to both sites with deployed and non-deployed systems as well as those sites having only non-deployed systems. The Treaty further contains a number of provisions fostering transparency, including, but not limited to biannual data exchanges and the sharing of telemetric information. Of special consequence for the cooperative provisions of the Treaty is the establishment of a Bilateral Consultative Commission (BCC) which meets at least twice annually and serves as a compliance and implementation body for the agreement. Either party can raise related concerns to the BCC.[13] Although there were fears that the Trump Administration's deploying of a submarine-launched low-yield nuclear weapons under the auspices of the government's arsenal modernization efforts could well threaten the renewal of New START, Vladimir Putin called for an unconditional extension of the Treaty in December 2020. In late January 2021, both Russia and the US articulated their willingness to extend the Treaty. On 4 February 2021, New START was formally extended until 5 February 2026. It is indeed serendipitous that the Treaty was extended a few short weeks prior to the recent chill between the Biden Administration and Russia.

Cooperation in Cyberspace: A Possibility?

Both Russia and the US have been involved in successful efforts to fight cybercrime and or cyberwarfare, although these have by and large been fleshed out within the broader contexts of other international cooperative efforts (BRICS/CyberBRICS; the Shanghai Cooperation Organization; the Budapest Convention, the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence, Growth in the Americas/América Crece. etc.). Moreover, the Soviet Union/Russia and the US have, over the course of the Cold War and recent decades, undertaken a number of impressive cooperative efforts in such areas as initiatives in the arts, academia, economics, security, and other domains. Given these achievements on both parts, one would naturally expect that cooperation in cybersecurity, and specifically in counter cyberterrorism would be at once mutually beneficial and feasible. The following chapter, however, will examine the problems that the two superpowers have encountered in attempts to undertake cybersecurity initiatives or to create a working cybersecurity regime.

CHAPTER IV:

FAILURES OF RUSSIA AND THE US IN FORMING A COUNTER CYBERTERRORISM REGIME

The previous chapter has examined the success of Russia and the US in participating in international cybersecurity initiatives. It has demonstrated that Russia has liaised both with the BRICS group and the Shanghai Cooperation Organization, although cybersecurity has been but one of a number of domains of cooperation. Similarly, the US has worked towards the development of cyber policies with both Latin America and the Caribbean, in initiatives which constitute but a part of a larger spectrum of cooperative efforts. The two superpowers, however, have failed in their attempts to develop sustained cooperation with each other, let alone to form a regime. Moreover, despite a number of cooperative efforts involving either Russia and the US and their respective allies, other international efforts between each superpower and other international alliances have proven difficult or impossible. This chapter will provide a counterpoint to Chapter III in that it will first briefly explore failed or problematical international efforts which involve either the G8 or NATO/EU. This example is chosen because both entities can now be deemed Russia's competitors in multiple domains, and in recent years, the US has had several situations which have strained its relations with its close allies. It will then present an overview of the failed attempts on the part of the two superpowers to enter collectively into counter cyberterrorism cooperative initiatives or to develop a regime to this effect.

Failed Possibilities: A Russian Perspective

One of the primary unsuccessful efforts in which Russia has participated is its involvement in G8. In 1997, Russia was invited to join the Group of Seven, or G7, a forum comprised of France, Germany, Italy, the UK, the US, Canada, and Japan, The G8 has an informal structure, lacking both a charter and a secretariat, and hence is not a formal institution. While the former G7 continues to meet on issues of international economics, the G8, with Russia included, focuses its efforts on other issues related to foreign affairs (Council on Foreign Relations, 2018). The Group is, in effect, a subset of G20, an economic council of the world's wealthiest nations. In 2009, the G20 summit in Pittsburgh was confronted by protests, both peaceful and violent, which decried corporate greed and the treatment of such non-sovereign nations as Tibet and Palestine, and which advocated for environmental concerns (Ian Urbina 2009) (Council on Foreign Relations 2018). At this summit, it was decided that inasmuch as a good number of the economies represented in G20 had witnessed considerable growth, the larger group would replace the G8 as the primary economic council of highly-developed countries. The role of the G8 would henceforth be that of a "steering group for the West." Japan would participate in a special capacity (Stepanie Lee and Alexandra Silver, 2014). Russia held the presidency of the G8 in 2006 and was elected to this role again in 2014. Russia's agenda for the G8, as released in 2014, included issues responding to its own political priorities. These included the fight against drug trafficking and terrorism, conflict resolution, disease management, and health security (European Parliament, Directorate General for Foreign Policies, 2014).

Among the expectations of membership in the G8 is that all participants must be democracies with highly-developed economies. The Kremlin was initially invited to join the Group upon the encouragement of several international leaders, most prominently President Bill Clinton. It was hoped that membership in the Group would encourage Russia along its road to democracy. Russia's membership, nonetheless, was contended throughout its tenure in the G8. Its backsliding towards autocracy, overall human rights record, and arms sales to and financing for Syria's Bashar al-Assad regime was contrary to the stance of other members of the G8 (Stephanie Lee and Alexandra Silver, 2014). The most contentious moment of fall was the annexation by Russia of Crimea, which the presidents of the European Council and European Commission condemned through a statement officially authored by the G7. The Statement argues that the annexation of Crimea would not only constitute a clear violation of the United Nations Charter, Russia's commitments under the Helsinki Final Act, the 1997 Treaty of Friendship, Cooperation, and Partnership between Russia and Ukraine, and Russia's obligations under the 1994 Budapest Memorandum (White House, Office of the Press Secretary, 2014). The Statement further stresses that, "In addition to its impact on the unity, sovereignty and territorial integrity of Ukraine, the annexation of Crimea could have grave implications for the legal order that protects the unity and sovereignty of all states" (White House Office of the Press Secretary 2014). Russia's failure to withdraw from Crimea and abort its occupation led to its ousting from the G8. Despite barring Russia from the Group until it changed its course, The G7 did not impose major sanctions on its former partner, unless Russia attempted to annex more of Ukraine. As Allison Smale and Michael D. Shear argue, the presence of Russia in the G8 had indicated cooperation between East and West, and its exclusion "raises new echoes of Cold War-style rivalry" (2014).[14] Russia, in turn, announced its intention to withdraw permanently from the G8 in January 2017. Upon its withdrawal, Russian Prime Minister Dmitry Medvedev stressed, "It is clear what this Group of Seven means without other major economies –Nothing!" (Tom Batchelor, 2017).

On 21 March, 2021, the G7 marked the seventh anniversary of the annexation of Ukraine by reaffirming its expulsion of Russia. It reiterates the essence of its earlier statement, yet adds other significant points, emphasizing:

> We condemn Russia's violations of human rights on the peninsula, particularly of Crimean Tatars. We call on Russia to respect its international obligations, allow access to international monitors, and to immediately release all those who are unjustly detained. We welcome in principle Ukraine's initiative to establish an International Crimean Platform to consolidate the international community's efforts on Crimea. We also firmly oppose Russia's continued destabilization of Ukraine, especially Russia's actions in certain areas of the Donetsk and Luhansk regions, disregarding the commitments it made under the Minsk agreements. The full implementation of the Minsk agreements is the way forward for peace. Russia is a party to the conflict in eastern Ukraine, not a mediator (Republique de la France, Ministère de l'Europe et des Affaires Étrangères, 2021).

The relationship between Russia and the G8 is but one sign of the ongoing distancing of its relations with the West. As mentioned earlier, the annexation of Crimea was part of a broader sphere of activities that include, but are not limited, human rights issues and support for the Bashar al-Assad regime, that demonstrate strong ideological and strategic differences between Russia and the EU and the US. Assuming the presidency of the G8 for the second time, Russia had placed on its agenda the fight against terrorism. Yet cooperation with theG8 to this effect never took place due to Western perceptions of its actions. The current state of affairs renders cooperation with Russia a most difficult venture.

Problematized Possibilities: A US Perspective

Russia's failure to cooperate with the G8 is not a surprise. It is based on ideological differences that will be discussed at greater length in Chapter 5. In contrast, the US and the EU should ostensibly be less problematic. Nonetheless, in recent years, issues have occurred which have reduced trust between the US and some of its closest allies. Although this has not yet led to failed cooperation, this future is becoming an increasing prospect.

An especially negative series of events occurred in 2013, when Edward Snowden, a former employee of the CIA and subcontractor to the National Security Agency (NSA), made unauthorized copies of classified documents from the NSA, which involved US espionage against its European allies. The documents involved massive surveillance activities by the US and the UK, which breached international codes of ethics and involved, among other activities, the monitoring of the phone calls, text messages, contacts, and daily activities of millions of individuals in the US and internationally as well as of the classified and private communications of world leaders and other politicians ("NSA Monitored Calls of 35 World Leaders," 2013). This led to internet companies around the world being forced to install systems that the NSA could not penetrate. Inasmuch as the NSA undermined Internet encryption systems, businesses around the world that depended upon the privacy of banking and medical data were hurt. Snowden also made it public that James Clapper, Jr., director of National Intelligence, had lied to Congress in March 2013 when he denied that the NSA was collecting data on millions of US citizens (*New York Times* Editorial Board, 2014).

Snowden's reports caused public outrage over the agency's abuse. Two US federal judges accused the NSA of having violated the US Constitution. Ultimately, President Obama forcefully indicted the NSA for invasion of privacy and ordered a revamping of its activities. On the other hand, Obama condemned Snowden's whistle-blowing actions, arguing that he should have discussed the information he had found through appropriate channels. On 1

January 2014, The Editorial Board of the *New York Times* decried US charges against Snowden and argued that Snowden had done his country a great service and that clemency was in order to bring him back from exile in Russia and that the accused should "[…] have the hope of a life advocating for greater privacy and far stronger oversight of the runaway intelligence community."

The Snowden Affair led to considerable distrust of US intelligence among the country's closest allies. On 14 October 2013, French President Hollande spoke to Obama, stressing that he felt "deep disapproval of these practices, which are unacceptable between friends and allies because they infringe upon the privacy of French citizens" (*Al Arabiya*, 2013). Hollande demanded an explanation that indicated exactly what information to this regard was available to Edward Snowden. The two leaders agreed to cooperate in assessing the scope of US surveillance activities.

Exchanges between France and the US continued. In 2015, reports reached Paris that the US had spied on three consecutive French presidents. In June of that year, Hollande phoned Obama to emphasize that such activities were unacceptable and were a threat to French security. French government spokesperson Stéphanie le Foll announced Hollande's plans to send a senior French intelligence agent to Washington for further discussions with US counterparts. She stated, "We find it hard to understand or imagine what motivates an ally to spy on allies who are often on the same strategic positions in world affairs" ("Obama Calls Hollande to Promise U.S. Is No Longer Spying on French President," 2015). In an additional phone call, Obama articulated that the NSA had ceased espionage activities against Hollande.

Similar altercations occurred between German Chancellor Angela Merkel and Obama. In October 2013, Merkel phoned Obama to express her outrage that US intelligence was monitoring her cellphone. Obama directly denied these allegations. Merkel further demanded that the US reveal the extent to which it was conducting surveillance activities in Germany.

White House Spokesman Jay Carney stated that “The United States is not monitoring and will not monitor the communications of the chancellor” (“Merkel Calls Obama about ‘US Spying on Her Phone,’” 2013). Carney failed, however, to state whether such surveillance had been conducted in the past. Germany demanded that the US must provide “an immediate and comprehensive explanation [of this] serious breach of trust” (“Merkel Calls Obama about ‘US Spying on Her Phone,’” 2013). Steve Evans of the *BBC* reported that the issue of state monitoring of phone calls had a special resonance in Germany. After all, Merkel had grown up in the German Democratic Republic, where the bugging of telephone communications of private citizens was a well-known and widespread occurrence.

Other close US allies expressed their indignation at the reports of US surveillance. Brazilian president Dilma Rousseff, in a speech at the UN, expressed her disbelief at US arguments that US interception efforts had been intended to protect nations against terrorism, drug trafficking, and organized crime. In 2013, she cancelled an official visit to Washington in protest of the NSA’s electronic interception of communications in her country, and most specifically, of her office. In turn, Mexico stressed that the spying on emails of two of its presidents, Enrique Peña Nieto and Felipe Calderón was unacceptable (“Merkel Calls Obama about ‘US Spying on Her Phone,’” 2013).

Together with the obvious fact that the US and its close allies, both in Europe and in Latin America, must rebuild trust, particularly in the domain of security, the repercussions of the Snowden Affair are far reaching. In July, 2020, six EU states and the US convened in Luxemburg to argue a challenge initiated by Austrian privacy activist Max Shrems who claimed that US laws governing the ways in which intelligence agencies can gain access to personal data from European Facebook users run contrary with privacy laws in Europe. Such a situation could have tremendous impact on Facebook and other companies and could greatly damage the transatlantic international economy (Kenneth Propp 2019, p. 1). The case examined the efforts of the US and the EU to reconcile privacy rights with national security, which have been ongoing for the past 20 years. Kenneth Propp argues:

> […] the tenor of the court's questioning during the July hearing suggests that this balance is at serious risk. The ECJ's judgment in the Shrems case, expected early next year, could lead to a diplomatic and legal confrontation between the EU's new leadership and a Donald Trump administration not well disposed toward the EU (2019, p. 1).

Propp stresses that global commerce is dependent upon the possibilities for both consumers and diverse industries to transfer personal data efficiently across national borders and that international access to personal data is key to recent technologies, among these big-data analytics, cloud computing, and artificial intelligence. In this realm, the US and the EU are each other's primary trade partners (2019, p. 2). Propp outlines major differences between US and EU concepts of data privacy.US privacy law provides limited restraints on the sending of personal data from the US to foreign countries, and furthermore encourages the free flow of such data. In contrast , the EU has instated what Propp dubs "border controls," which regulate data transfers from Europe and provides that European personal data may only be sent to a third country "if there is a legal arrangement in place to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined" (("Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)" (Chapter V, Article 44, np).

Propp looks back to the period between 1998 and 2000, when the US developed the International Safe Harbor Privacy Principles. These principles included 1) Notice, whereby individuals must be informed about how their data is being collected and used; 2) Choice, whereby individuals must be able to opt out of the collection and transfer of their data to third parties; 3) Onward Transfer, which specifies that transfer of data may only be made to other organizations, following adequate data protection principles; Security, in which it is specified that reasonable efforts must be undertaken to prevent the loss of data which has been collected; Data Integrity, which specifies that the data must be both reliable and relevant to the purposes for which it was collected; Access, which provides individuals with the opportunity to access information that has been collected about them and make appropriate corrections or requestion deletion of incorrect information, and Enforcement, which stipulates that there must be an effective means whereby these rules can be enforced (US Federal Trade Commission, 2015). In July 2000, the European Commission determined that Safe Harbor met the requirements of the EU, and Safe Harbor went into effect. In the wake of the Snowden affair, however, Shrems argued that Safe Harbor did not protect the data that had been entrusted to Facebook. This led to the decision that a company is not obliged to defer to US surveillance requests and to a further strengthening of individual privacy rights. Although the EU and the US eventually agreed upon a revised Privacy Shield, the extensive role that the European Court of Justice has played in matters of individual data security and privacy has been most frustrating to the US. One can only speculate as to whether the situation will become more harmonious under the Biden administration.

Another recent series of events that has caused tension between the US and its allies in the domain of security involves the controversy over Turkey's purchase of an air defense system from Russia. This purchase was strongly condemned by the Trump administration. Matthew Lee asserts that the sanctions were imposed at a particularly sensitive moment in which relations between Turkey and the US were especially strained due to Turkey's actions in Syria. This situation was further worsened by the recent conflict between Armenia and Azerbaijan.[15] As Lee explains, these sanctions were required in accordance with a US law passed in 2017, titled the Countering American Adversaries through Sanctions Act (CAATSA), which required a "pushing back" on Russia if a US administrated found a substantial reason (Matthew Lee, 2010). Nonetheless, as Lee stresses, this is the first time that the law had been employed against a US ally. Earlier, the US had removed Turkey from the F-35 stealth fighter development and training program over the purchase, arguing that the "System is incompatible with NATO equipment and a potential threat to allied security" (Matthew Lee, 2020). Secretary of State Mike Pompeo urged Turkey to resolve the problem in conjunction with the US, stressing:

> Turkey is a valued ally and an important regional security partner for the United States, and we seek to continue our decades-long history of productive defense-sector cooperation by removing the obstacle of Turkey's S-400 possession as soon as possible (Matthew Lee, 2020).

Turkey's foreign ministry condemned the US's decision and threatened that "Turkey will take the necessary steps against this decision, which will inevitably affect our relations in a negative way, and reciprocate in a way and time it sees fit" (Matthew Lee, 2020). Russia's foreign minister Sergei Lavrov supported Turkey's stance in this issue and described the sanctions as evidence of American arrogance, stressing that they would "hurt US. standing internationally" (Mathew Lee, 2020).

Neither the Snowden affair nor the recent falling out between the US and Turkey can be deemed total failures in terms of international security. Nonetheless, they have weakened considerably US ties with both the EU and NATO in matters of security. In both cases, what is most at stake is a considerable reduction in trust, which the US had worked hard to build with its allies over the course of many years. Trust is a key component in the formation of regimes, and as will be demonstrated below, the lack of trust is one of the primary impediments to the creation of a counter cyberterrorism regime by Russia and the US.

Russia and the US: Failures in Cybersecurity Cooperation

Despite a number of successful collaborative efforts between Russia and the US, among these the Treaty on the Non-Proliferation of Nuclear Weapons, the uranium agreement, and New START, no agreement has been successfully developed between the two superpowers. An attempt was made between 2002 and 2006, yet it stagnated, a fact that is most disconcerting in light of other successful joint initiatives over the years. Indeed, it should have proven to be successful given what should be the urgent relevance of counter cyberterrorism to both states. This attempted initiative was led primarily by the scientific communities of both countries, and early on pointed optimistically to the possibility of joint efforts between the two superpowers by means of track-two diplomacy.

The initiative was limited, but noteworthy and involved a series of three workshops held in Washington, D.C. in 2002, 2004, and 2006, which focused on counterterrorism. The workshops are discussed here under failed initiatives due to the fact that they were abandoned in 2006. Nonetheless, they will be revisited in the Conclusion to this thesis as an initiative that clearly demonstrates a promising course for the future. The workshops were sponsored by the US. National Research Council of the National Academies and the Russian Academy of Science. Cyberterrorism was never the focus of the workshops, yet it did come to the forefront in the 2006 edition. The 2006 Workshop was titled "Countering Urban Terrorism in Russia and the United States," and it included presentations on the relationship between cyberterrorism and urban terrorism and the role of science and technology in counter terrorism. Of special consequence was a presentation by the a presentation by the Russian/US Working Group on Cyberterrorism Issues, a consortium that had developed over the course of the previous conferences. The presentation provided updates on activities within the two countries devoted to preventing Cyberterrorism. The Working Group was comprised of Anita K. Jones, a professor of engineering and applied science at the University of Virginia; Lewis M.

Branscomb, a professor emeritus of Public Policy and Corporate Management of the John F. Kennedy School of Governance of Harvard University; Linton Wells III of the Wilson Center; Michael Wolin of Nobel Insights; A. Chelsea Sharber, Senior Program Associate of the National Research Council; Igor Fedorov (affiliation unknown); Nikolay V. Medvedev of the Saint Petersburg Polytechnic University, and Yuri K Shiyan, director of the Russian Office for North American Scientific Cooperation. The Group visited the National Cyber Security Division of the Department of Homeland Security and heard briefings by the CERT (Computer Emergency Response Team) Coordination Center of Carnegie Mellon University and the National Academies Computer Science and Telecommunications Board (Anita K. Jones et al, 2006, pp. 9-13).

The priorities for the future identified by the Group include 1) the creation of cooperative and complementary research programs to develop new principles, methods, and tools aimed at building reliable systems, and 2) the exploration of the most effective approach for developing national and international policy and law for cybercrime and cyberterrorism (Anita K Jones et al, 2006), p. 11). The Group believed that the rate of research progress to develop more dependable and robust systems is far short of what is needed. Further, without metrics to quantify both costs and benefits of reducing vulnerability to cyberattack, markets for those tools will continue to be weak for developing national and international policy and law for cybercrime and cyberterrorism. In order to develop policy, it is important to examine the need for a common glossary of terms for international use in laws and regulations, jointly developed by legal and technical experts, and to explore how the academies can facilitate the solution of these problems. Legal and regulatory structures for suppressing cyberattacks are fragmentary, inconsistent in terms and language used, and incompatible across national boundaries. Progress to rectify these shortcomings is urgent (2006, p. 11). Other suggestions by the group involved exchanges and education between the two countries. Topics to be covered in such trainings would be the development of a security policy based on international and national standards; the use of international standards to analyze information security risks; the development of a network traffic security policy; the application of techniques of information security identification and the elimination of information security threats; the implementation of information security based on international and national standards; the identification of security risks; the modeling of attacks and protection technology, and the auditing of information security systems (2006, p, 12). The Working Group further reported on the six-year program at Baumann Moscow State Technical University, which provides an interesting model for cyber-education and cyber-training. It firmly believes that academic exchanges are the best way to get experience with alternative curricula for cybersecurity. Summer internships and programs for students (graduate and undergraduate), instructors, and researchers are included in this possibility (2006, pp. 12-13).

Three of the American participants in the Working Group also presented a paper on cybersecurity and urban terrorism at the Workshop. Although their paper focused exclusively on the US, examining such areas as emergency response plans for urban areas; timely response; preplanned and coordinated operations; access to critical information, and assured communication, they conclude by referencing Russia/US efforts. They stress:

> Our working group believes that Russia and the United States share this problem. The governments in both countries need to think through how to avert cyberattacks directed at emergency response activities. Policies, plans, and budgets need to be put in place to assure the functioning of emergency resp (2006, p. 24).

Despite the highly laudable efforts of the Working Group, it appears to have disbanded following the 2006 Conference.

The possibility of Russian/US cooperation has, moreover, not gone unnoticed by think tanks. In 2010, a paper published by the New York City-based EastWest Institute, an international organization, explored the possibility of and difficulties involved in US-Russian cooperation on cyber-diplomacy. Authored by Franz-Stefan Gady and Greg Austin (2010), the report examined the prospect from a number of closely related angles, among these infrastructure technology; cybercrime cooperation with Great Britain; the work of OSCE and the Cyber Warfare Law, and the efforts of NATO. The paper stresses that, despite a 1998 declaration of the two powers' interest in joint leadership of a global response, Russia and the U.S. have been acting as enemies rather than as allies in the realm of cybersecurity. Gady and Austin point out cooperation efforts over the course of the past 20 years, which suggest that reservations on both parts can be overcome. For example, the countries championed the implementation of monitoring measures, which garnered strong international support, to prevent a Y2K missile launch, and, more recently, they also jointly undertook encryption efforts for th Moscow-Washington hotline (Gady and Austin, 2010, p. i). As Gady and Austin explain, in 2009, the "Obama administration announced that it would take cybersecurity to a new level, which, at the time, appeared to open doors to an expansion in Russian-US cooperation" 2010, p. (i).

Despite recognition of the importance of joint efforts between Russia and the US in combatting cyberterrorism, relations between the two superpowers deteriorated greatly when allegations were made of Russian meddling in the 2016 US elections. US intelligence and former Special Counsel Robert Mueller found evidence of extensive contact between the Trump campaign and Russia in order to assure a smear campaign against democratic candidate Hillary Clinton. A 17 December 2018 US Senate Intelligence Committee report presented evidence that Russia used Facebook, Twitter, YouTube, Tumbir, Instagram, and PayPal in its efforts. Committee Chairman, a Republican senator from North Carolina argued that Russia aggressively "sought to divide Americans by race, religion and ideology (US Senate Intelligence Committee 2018). He underscored that it was particularly troubling that Russia's activities had not ceased. He called for "an increase in information sharing between the social media companies who can identify disinformation campaigns and the third-party experts who can analyze them" (US Senate Intelligence Committee 2018).

On the tail of the election meddling the US was notably displeased by Russia's proposal in 2018 for a UN Open-Ended Working Group (OEWG) on issues of international security and cyberspace. The Proposal ran contrary to US desire for a Western Hemisphere cooperation to counter cybercrime. The US deemed Russia's actions an affront against a proposal for a Group of Governmental Experts (GGE) that it had proposed, which would study the relationship between international law and state action in cyberspace, with the intention of promoting compliance with existing norms. Alex Grigsby explains that by advocating for an OEWG (open-ended working group), Russia attempted to show itself as an advocate of democratic participation and inclusivity, framing itself as a defender of the rule-based international order and committing to multilateral solutions to international challenges. Its resolution stripped itself of language drawn from the Shanghai Cooperation Organization's International Code of Conduct on Information Security, thereby making its texts less offensive to members of the General Assembly given that the Shanghai Organization's code undermines rights to the protection of online activity. The US and its allies strongly criticized the Russian proposal inasmuch as it "cherry-picked" language from previous Group of Experts (GGE) reports and accused Russia of being divisive inasmuch as it put forth a proposal that would not gain a consensus in contrast to those resolutions made on the topic during the previous two decades. It further indicted Russia for using language from a controversial 1981 General Assembly proposal that claims that states must "abstain from any defamatory campaign, vilification or hostile propaganda, which could interfere in normal state affairs (Alex Grigsby 2018).

Recent months have been especially devastating for cooperation between Russia and the US in virtually any capacity. In early March, 2021, the US levied sanctions against Russia for the poisoning of journalist Aleksei A. Navalny. Shortly thereafter, a US intelligence report dated 15 March 2021 alleged that Russia had further meddled as well in the 2020 elections, with a number of Trump's top lieutenants supporting claims against Joe Biden made by pro-Russian Ukrainian figures. The report further provided evidence that Putin either directed or supported the election meddling so as to guarantee Trump's victory. It did not, however, find any evidence to support claims that Russia had influenced US voter registration, the casting of ballots, the tabulation of votes, or the reporting process. Finally, the Report found that China had not had any interest in supporting either side, side, and thus, unlike Russia, it engaged in no election meddling (US National Intelligence Council, 2021). Two days following the release of this report, President Biden fueled the growing rift between Moscow and Washington during a 17 March ABC Television Interview with political commentator George Stephanopoulos, in which the President characterized his Russian counterpart as a murderer. He further threatened that Russia would pay for interference in the 2020 US elections. Putin's response to the interview was extremely direct and strong; he recalled the Russian ambassador to Washington to discuss the ramifications of the situation. This is the first time Moscow has recalled an ambassador to the US since 1998, an act of protest against the US invasion of Iraq. Konstantin I. Kosachev, the head of the Foreign Affairs Committee of Russia's upper house of Parliament posted on Facebook that, in light of Biden's remarks, "Any expectations for the new U.S. administration's new policy toward Russia have been written off by this boorish remark" (Anton Troianovsky, 2021). Arguably, Russia/US relations are at an all-time low for the post-Cold-War era.

The following chapter will apply Constructivist theory and the newly defined concept of Cooperation Culture to examine the findings articulated in the discussions of Chapter III and the current chapter. The goal of Chapter V will be explanatory in nature, to elucidate the factors that have rendered the formation of a counter cyberterrorism regime between Russia and the

US most difficult. This discussion will be followed, in the conclusion, by a note of optimism, exploring tactics and postures that could lead to the building of trust between the two superpowers and pave a road to cooperation in the fight against cyberterrorism, a threat that could have a catastrophic impact on either Russia or the US.

CHAPTER V

ANALYSIS OF IMPEDIMENTS TO THE ESTABLISHMENT OF A CYBERSECURITY REGIME BETWEEN RUSSIA AND THE US

The impediments to the formation of a counter cyberterrorism regime by Russia and the US are multidimensional. From a constructivist perspective, they interface the strategic approaches of both countries with deeper socio-cultural issues. Essential to the development of a cooperative initiative is an understanding of the very nature of cybersecurity, which is notably different for Russia and the US. Among the primary concerns that separate the two nations in this regard are their divergent perspectives on Internet access and online freedom of expression, particularly of viewpoints that may be distasteful to the state and their overall views of the right to privacy and human rights. Indeed, the primary cyber divide that separates them is ideological, and these divergent ideologies are, in part, shaped by norms and culture (Hoyoon Jung 2002, p. 2). The following discussion will first present a brief examination of the strategic cultures of both countries, with emphasis on the employment of the concept in the domain of regime formation. It will then revisit several agreements discussed in Chapters III and IV and few others to analyze the choices made by Russia and the US in their respective cyber alliances. These alliances will serve an explanatory purpose, to clarify the impasse that the two superpowers have struck in any attempt to develop sustained cooperation in the fight against cyberterrorism.

Strategic cultures of Russia and the US

Whether today's Russia, the Russia of the tsars, or the largest republic of the Soviet Union has always been autocratic. Referring to imperial Russia, Richard Wortman explains, "The imperial system, it is true, was built on an authoritarian political culture that had evolved in Muscovy, and many of the earlier patterns would resurface during the evolution of the Soviet state […]" (1987, p. 197). In post-Soviet Russia, one notes a continuation of such an authoritarian climate. Norbert Eitelhuber offers an explanation for such a history of authoritarianism by explaining it in part through a discussion of Russia's historical tendencies in "threat perception" (2009, p. 5). As Eitelhuber clarifies, Russia has suffered through a long history of being invaded, conquered, and/or dominated, from the Kievan Rus, who were subjugated to the Golden Hordes for some 200 years, to a number of attacks on Moscow (Tatars in 1571, the Poles in 1610, Napoleon in 1812). Although Russia ultimately remained victorious in the struggle against Napoleon, it suffered greatly from the invasion. In the 20th century, one need only mention the Japanese attack on the Russian navy base at Port Arthur (1904), the Polish invasion of 1920, and the ravages of two world wars. According to Eitelhuber, these events "left deep scars on Russia's collective memory" (2009, p. 5). Russia, moreover, lost its dominance over a large portion of the territory of the Soviet Union when the latter collapsed, and separatist movements in the North Caucasus have threatened its unity (Eitelhuber, 2009, p.6). Russia has become a highly ethnocentric culture and is especially suspicious of its closest neighbors. According to Eitelhuber, Russia's persistent history of autocracy has been a response to such threats. He stresses, "Given the state's vast size and multi-ethnic nature, autocratic leadership seemed to be the type of governance that was best suited to cope with the wide range of external and internal threats that cropped up throughout Russian history […]" (2009, p. 6). Eitelhuber links the above considerations to Russia's quest to become a great power, a goal to which it progressed gradually, over time.[16] Eitelhuber's discussions offer insights into the shared experiences that impact behavior on the level of international relations in general, and most specifically, on that of security culture.

In what concerns the above perspective, Ivor Wiltenburg underscores that Russia's authoritarianism stems from a "historical and enduring sense of insecurity," and adds the "[…] "Russia considers itself a great power and demands to be treated as such (2020, p. 8). According to Wiltenburg, resources reflecting power and the recognition of other states are essential to its status as a great power (2020, p. 8). Wiltenburg stresses that recent events that have contributed to Russia's perception of threat include the Iraq invasion of 2003, the Ukrainian revolution of 2004, Arab Spring, Western intervention in Libya, and Russian protests following the 2011 elections, all of which suggested a Western agenda to destabilize Russia and force governmental change (2020, p. 8). All of these events have contributed to what R Rashed Uz-Zaman would describe as the "documentary" level of culture (2009, p. 70), and which, in turn, is a defining element of strategic culture.

In contrast to Russia, the US, since the Revolutionary War, has never suffered a war on its own turf. Hence, the 9/11 attacks were so disconcerting to Americans. The US has never been the target of severe threats from its neighbors. An exception to this trend has been the US embargo of Cuba in the wake of the onset of the Castro regime and the Cuban Missile Crisis. Like Russia, the US has been an expansionist nation. Yet this has not been out of fear of its neighbors or minorities. Rather, a driving force for the US's desire to dominate the land stretching from the Atlantic to the Pacific was the ideology of "manifest destiny," which was predicated upon the beliefs that the (European) American people, their ideology, and their sociopolitical structure were of particular righteousness and must be spread; that the US must claim the West and remake it in the image of the (colonize) East, and that this expansionism was the nation's essential destiny.[17]

Dima P. Adamsky relates manifest destiny to US strategic culture and examines the nation's strategy to maintain its power and influence. Adamsky argues that, for the US, "Self-efficacy dictates a strategy to shift the conflict into those arenas where one enjoys an inherent advantage over one's enemy" (2008, p. 38). Adamsky explores how the founding fathers of the US believed that America represented a "new beginning, and that this perspective contributed to a "national identity based on liberal, democratic, Protestant and capitalist principles. Individual freedom, pragmatism, and rationalism formed the cornerstone of the new society" (2008, p. 28). She stresses:

> The capitalist economy, liberal political structures and a strong spirit of exploration produced a belief that as nature could and should be understood, potentially almost any problem can be solved. Optimistic entrepreneurship became a value in all fields of American social activity and created a society based on notions of efficacy, rationalism and pragmatism. Compounded by repeated success, it produced a romantic engineering creed that viewed social and security problems as essentially mechanical in nature and, consequently, consistent with the logic of man-made machines (2008, P. 38).

Although Adamsky's argument clearly focuses on conflict and war, much of it can be implied to other spheres of US life. When one considers information science, the aforementioned remark by Julien Nocetti comes to mind. For the US, a primary goal of cyber security is to protect an area in which, to cycle the argument back to Adamsky, "the US enjoys an inherent advantage." As Nocetti argues, Russia perceives the US as deeming cyber security to be located in a primarily techno-logical domain, while for Russia, the concept is broader and more philosophical (Julien Nocetti" (2015, p. 126).

The strategic cultures of Russia and the US are not completely inimical—after all, both are expansionist countries, expect recognition as superpowers, and seek the all that is required to maintain this status--, nonetheless, the marked differences in their perception of their respective neighbors and citizens, which are the result of a sense of insecurity on the part of the Russians and of entitlement on the part of Americans, render attempts to build a joint counter cyberterrorism regime extremely challenging.

Russia’s Success in International Cooperation to Combat Cyberterrorism—an Analysis

In the Goa BRICS Summit of 2016, which was titled “Building Responsive, Inclusive and Collective Solutions,” a declaration was released which dealt primarily with areas of economic cooperation. Although it fails to mention the word “cyber,” there are 24 references to “terrorism.” The concept of cyberterrorism is implied through the notion of “misuse of Information and communications Technologies (ITCs)” by terrorists (BRICS 2016, 59). Specific references are made to terrorist activities in Afghanistan, Iraq, and the Levant (2016, § 16 and 61). The Declaration condemns recent terrorist activities against the BRICS nations, and specifically mentions India. BRICS affirms its commitment to “[strengthening] cooperation in combating international terrorism both at the bilateral and at international fora” (BRICS 2016, (§ 57). It acknowledges the efforts of the BRICS Joint Working Group on Counterterrorism, which promises to “[…] further promote dialogue and understanding among BRICS nations on issues of counter terrorism, as well as coordinate efforts to address the scourge of terrorism (2016, § 60).

The GOA Declaration includes a call for the United Nations, the African Union, and other regional and international partners to cooperate in addressing this problem as well as issues of post-conflict resolution and development efforts (BRICS 2016, § 20). It stresses that terrorism, together with BREXIT, refugee flows, and geopolitical conflicts at large have “added to the uncertainty of the global economy” (BRICS 2016, § 24). BRICS makes that plea that all nations:

> […] adopt a comprehensive approach in combatting terrorism, which should include countering violent extremism as and when conducive to terrorism, recruitment, movement of terrorists, including Foreign Terrorist Fighters, blocking sources of financing terrorism, and countering misuse of the Internet including social media by terror entities through misuse of the latest Information and Communication Technologies (ICTs). Successfully combating terrorism requires a holistic approach. All counterterrorism measures should uphold international law and respect human rights (BRICS 2016, § 59).

BRICS further urges all member states of the UN member states to “undertake effective implementation of relevant UN Security Council Resolutions”:[and to] “expedite the adoption of the Comprehensive Convention on International Terrorism (CCIT) in the UN General Assembly without further delay (2016, § 61).

In the entire Goa Declaration, only four references are made to human rights. The first is couched with other UN mandates, namely maintaining international peace and security and advancing global development (2016 § 7). It stresses that all counterterrorism efforts should uphold international law and respect human rights (2016, § 59). In what concerns the cyber realm, BRICS “[reaffirms] that ICT expansion is a key enabler for sustainable development, for international peace and security and for human rights” (2016, § 64). Finally, human rights are mentioned in the context of right to privacy. The Declaration includes an ungrammatical and awkward paragraph stating the importance of “universally accepted norms and principles of international law, including the Charter of the UN; in particular political independence, territorial integrity and sovereign equality of States, the settlement of disputes by peaceful means, non-interference in internal affairs of other States as well as respect for human rights and fundamental” in the “peaceful, secure, and open and cooperative use of ICTs (2016 § 65).

One of the priorities of Brazil's 2019 chairmanship of BRICS was "economic growth for an innovative future" (BRICS "The Declaration of the BRICS Communications Managers Meeting held in Brasília, Brazil in August, 2019. The BRICS nations committed to cooperating with each other in digital connectivity; increasing connectivity and broadband access to digital technologies, and digital innovation (BRICS Communications Managers 2019, § 6.1 and 6.2). The sole reference to security emphasized BRICS intention to develop "enhancing robust security frameworks in digital economy to assure that the benefits arising from it are widely shared (2019, § 6.3).

In November 2020, China ratified BRICS' Counterterror Strategy which focused on an effective fight against cross-border terror, thereby hindering its ability to shield Pakistan and Pakistan-based terror groups and operatives. This ratification indicates a strengthening of India's demand that BRICS put forth a united front against its threats from Pakistan. The strategy demands "a rejection of double standards on countering terrorism and extremism conducive to terrorism (Dipanjan Roy Choudhury, 2020). At the top of the agenda of India's 2021 presidency of BRICS are counterterror strategy and multilateral reform. Concern has been voiced by India that China may, despite its ratification of the BRICS Counterterror Strategy of 2020, may continue to protect Pakistan. As Dipanjan Roy Choudhury stresses, "China's intransigence has often made it difficult to designate terror-operatives at various international for a" (2021). Hence, the most controversial counterterror issue facing BRICS at this time is lack of trust between India and China to this effect. This issue does not involve Russia. Nonetheless, its role in the tense situation cannot be underestimated.

Zeesham Munir and Raju Keshari describe India and China as emerging powers and Russia as a state that is "slowing stirring to regain its superpower" (2018, p. 94). They point out that, while Russia and India have enjoyed a long-term friendship, the same is not the case for China and Russia or India and China. They argue that Russia's cooperation with China in both BRICS and the Shanghai Cooperation Organization (SGO) has been at once cooperative and challenging. Although both Russia and India are “wary of China’s growing influence” and have adopted “policies of conciliation rather than confrontation,” the three countries are interdependent for their respective growth (Zeesham Munir and Raju Keshari, 2021, p. 95). Russia, moreover, is a force to be reckoned with by both New Delhi and Beijing, inasmuch as it supplies military products and services to both countries. As Munir and Keshari stress, “This status gives Russia the possibility to assume a more visible role in balancing out relations between India and Chian (3028. P. 105).

The BRICS conventions and declarations mention both human rights and the right to privacy for individuals, two issues that are contentious for Russia as a closed society. Nonetheless, these terms are expressed in highly generalized and relatively vague terms. There are sweeping statements such as “All counterterrorism measures should uphold international law and respect human rights” (BRICS 2016, § 59) which provide no specific details or requirements. When right to privacy is mentioned in the GOA Declaration, it is expressed as a mere afterthought to a litany of charges to the UN (2016 § 65). On at least one occasion, it is mentioned in a clumsy, run-on sentence. The ungrammaticality in English of the sentence undermines the strength of the statement (BRICS 2016, § 65). Human rights and the right to privacy appear to be afterthoughts to BRICS declarations and conventions, or appear therein simply to address UN expectations. Thus, the wording of these documents provides relatively little threat to Russia.

Of greater importance to Russia’s successful part in BRICS agreements is the very nature of the countries involved. Brazil, India, South Africa, and, to an extent, China, can be deemed emerging economies, presenting far less of a threat to Russia than the US or the EU. Moreover, it is able to divide and conquer, to foment mutual distrust between India and China through its military trade with both. This “keeps the pot simmering,” and discourages any quest for power on the part of India or China within the confines of BRICS. It further dissuades a strong political or economic allegiance between China and India. Colin S, Gray would likely argue here that this tactic speaks to Russia's might well argue here that this tactic speaks to Russia's "aspiration for self-characterization" as a superpower (2002, p. 22), and its desire to be recognized as such. This strategy on Russia's part recalls Bradley S. Klein's argument that strategic culture as a framework can be deployed to examine disjunctions between an actor's official rhetoric and their operational policies (1988, p. 136). For Russia, the other CRICS countries must not have easy access to its potential status, and its behavior attests to this underlying concern. It is especially significant to note that similar dynamics are at play within the SCO.

The key roles that Russia and China play in the SCO is reflected by the fact that the originals of a number of the group's declarations are authored in Russian and Chinese, with both languages carrying equal weight (Shanghai Cooperation Organization, 2009, Article 12, § 5). A 2009 Agreement among the nations of the SCO on matters of information security was signed. The language of the document is clearly anti-US in that it lists, among other threats to cybersecurity, "the use of the dominant position in the information space to the detriment of the interests and security of other States (2009, Article I, § 4). According to the Agreement, the main areas of cooperation include, but are not limited to identifying, agreeing on, and implementing necessary collective measures to ensure international information security; establishing collective measures to develop international law to curb the proliferation of information weapons; countering threats of using ICTs for terrorist purposes, and elaborating and building joint confidence-building measures to ensure international information security (2009, Article 3). According to the agreement, each party maintains the right to protect the information resources and critical structure of its State "from illicit use and unauthorized interference, including cyberattacks" and promises not to use such measures against another member state (2009, Article 4, § 3). Annex I of the Agreement defines the terminology used in the foregoing document. Annex II provides a list of major security threats in the information space. Together with such obvious threats as information terrorism, information crime, and "the dissemination of information harmful to the sociopolitical and socioeconomic systems, spiritual, moral and cultural environment of other States" (2009, Annex 2, together with promoting the ideas of terrorism, separatism, and extremism, this dissemination of harm (2009, Annex II, § 5), such dissemination of harmful information is characterized by:

> […] the appearance and replication of information in digital form (radio and television) and other mass media on the internet and other information exchange networks that: distorts the perception of the political system, social order, domestic and foreign policy, important political and social policies in the State, spiritual, moral and cultural values of its population […] (2009, Annex II, § 5).

The above reference is of particular consequence. It is clear that the Agreement is contradictory to any notion of freedom of speech and squelches the expression of dissent through any electronic means, including social media. It can further be read as extremely ethnocentric by virtue of its mere mention of the "spiritual, moral and cultural values of [a state's] population." This alone Appendix II, moreover, reiterates the main text of the agreement which views as an information threat the use of dominant position in the information space to the detriment of others. Although it further clarifies this statement in terms of the uneven international balance in access to the information realm, the role of the US as world internet leader is clearly implied as a threat ((2009, Annex II, § 5). As can be expected, inasmuch as the Agreement did not constitute a proposal to be put forth before the UN, there is no mention whatsoever of human rights or individual liberties. The verbiage of the SCO's 2009 agreement is thus in stark contrast to Western agreements of the like.

The SGO agreement thus attests to Russia's prevalent images and mental constructions that Adda B. Bozeman deems the result of historical and experiential processes (1976, p. 77). Strategically, Russia has been able to enter into an agreement with nations that do not pose a threat to its need to remain authoritative. This is clearly the opposite of any potential agreements with the West/

"The International Code of Conduct for Information Security" submitted to the UN General Assembly by China, Russia, Tajikistan, and Uzbekistan in September 2011 and in a revised version of January 2015 is a proposal that most decisively evidences the sharp divide between the SCO and the West (United Nations General Assembly, 2012 and 2015).[18] The first pledge articulated in each version of the proposed "Code of Conduct is:

> To comply with the Charter of the United Nations and universally recognized norms governing international relations that enshrine, inter alia, respect for the sovereignty, territorial integrity and political independence of all States, respect for human rights and fundamental freedoms and respect for the diversity of history, culture and social systems of all countries (United Nations, 2012, "Code of Conduct," § and United Nations, 2015, § 1).

In this respect, both submissions of the proposed Code of Conduct: mirror very closely the verbiage of the aforementioned Agreement upon the participants of the NCO. Paragraph c of the 2011 version further recalls the agreement. It calls for a curbing of the dissemination of information that "incites terrorism, secessionism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment" (2012), by curbing the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment" (United Nations General Assembly, 2012, "Code of Conduct," § c). This paragraph is significant in that, albeit earlier on there is a reference to "terrorist and criminal activities," the actual agent of the dissemination of such insightful information is left ambivalent. It could refer either to terrorist groups or operatives or to other nation states. Like in the 2009 Agreement, the reference to “spiritual and cultural environments” could have ethnocentric and nationalistic undercurrents. The paragraph, however, is somewhat softened in that it eliminates the word “moral.” In the 2015 draft of the “Code of Conduct,” the reference to “other countries” is eliminated, and the directive involves “information that incites terrorism, separatism or that inflames hatred on ethnic, racial or religious grounds” (United Nations General Assembly 2015a, “Code of Conduct, § 3). Arguably, the most blatant change between the two versions of the “Code of Conduct” involves rights and freedoms in information space. In the 2011 version, the freedom to search and disseminate information was subject to “relative national laws and regulations (United Nations, 2012, “Code of Conduct,” § f). In the 2015 version, this paragraph was completely reworked. According to the new version, an individual should have the freedom to seek, receive and impart information, all the while

> […] taking into account the fact that the international Covenant on Civil and Political Rights (article 19 attaches to that right special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary (United Nations General Assembly, 2015a, “Code of Conduct,” § 7).

The unified position of the SCO was thus one which favored state sovereignty and state control over the Internet. As mentioned earlier, the proposed “International Code of Conduct for Information Security” was put forth “[…] to achieve] the earliest possible consensus on international norms and rules guiding the behavior of States in the information space (United Nations General Assembly, 2012, “Letter Dated 12 September 2011”). The revised version of the Code was intended “[…] to push forward the international debate on international norms on information security, and help forge an early consensus on this issue” (United Nations

General Assembly 1015, “Letter Dated 9 January 2015”). The proposed Code remains contested. Susan McKune argues:

> The narrative of the Code emphasizes state sovereignty and territoriality in the digital space above all else, and is dominated by intelligence, national security, and regime stability imperatives. Perhaps most worrisome, trends embodied by the SCO and reflected in the Code itself suggest a strategic revisionism on the part of the SCO states towards international human rights law (Susan McKune 2015).[19]

McKune further asserts that, according to the verbiage of the Code, the so-called rights of an individual in the offline and online environments are “only those in existing domestic policies and practice” (Susan McKune 2015). She concludes her in-depth analysis of the Code by arguing that any claims that the Code is “consensus, either through “the support of or the silence of the international community, may erode protections for human rights guaranteed under international law” (2015). Although Russia and China indeed have their differences in a number of political and economic issues, they stand united in their endorsement of the notion of the extension of national sovereignty and control over cyberspace. In this respect, Russia’s cooperation with the SCO was fruitful in making a strong case internationally for this position. Once again, as in the case of BRICS, Russia was able to behave in accordance with its own particular (national!) way of life (Uz-Zaman 2009, p. 70). Little or nothing has occurred within the context of the SCO to interrogate its need to remain a closed society.

The US’s Success in International Cooperation to Combat Cyberterrorism—An Analysis

The Tallinn Manual on the International Law Applicable to Cyber Warfare (22013) is more of an academic study than a binding convention or agreement. It is intended to investigate how international law can be applied to cyber warfare and other cyber conflicts. Under the editorship of US, a professor of law at the US Naval War College's Center for International Law in Stockton, CA and editor-in-chief of an Oxford University Press Lieber Series, sponsored by the Lieber Institute for Law and Land Warfare, *The Tallinn Manual* appears to contradict a good number of the driving human rights principles of Western discourse on cybersecurity. Nonetheless, it is essential to recall that the scope of the manual is not cyberspace at large, rather it focuses on states of conflict and war. Its primary subdivisions are International Cyber Law; the Law of Cyber and Armed Conflict; Conduct of Hostilities; Certain Persons, Objects, and Activities; Occupation, and Neutrality. The *Manual*'s first reference to human rights stresses that a state may "restrict or protect (in part or in whole) access to the Internet, without prejudice to applicable law, such as human rights or international telecommunications law. The fact that cyber infrastructure located in a given State's territory is linked to the global telecommunications network cannot be interpreted as a waiver to its sovereign rights over that infrastructure" (Michael N. Schmitt, 2013, p. 17). A later reference to similar issues appears in the context of an occupying state. According to the *Tallinn Manual*, an occupying state may "curb the freedom of expression and of the press in cyberspace, despite laws to the contrary, as necessary for its security" (Michael N. Schmitt, 2013, p. 243). This includes preventing the use of electronic media by resistance groups to organize and network. An occupying state may also "take measures outside existing law if its computer networks outside occupied territory fall victim to cyberattacks launched from occupied territory (2013, p. 243). At a first glance, it may appear that the *Tallinn Manual* is not that distinct from the bids to sovereignty present in the "International Code of Conduct for Information Security." Afterall, both take into account a State's sovereignty over the Internet. Nonetheless, it is essential to recall that the *Manual* establishes conditions for warfare. Its primary context is that of *casus belli*. It is essential to compare the positions of the NATO partners that subscribed to the *Tallinn Manual* with those of the "International Code" outside of the context of war or cyberwarfare. In order to better understand how the US is behaving in international cyber concerns, it is necessary to contrast its position as articulated in the *Tallinn Manual* with those put forth in a less bellicose context.

At its summit in Warsaw in July 2016, NATO issued a cyber defense pledge. It confirmed its commitment to enhancing the cyber defenses of national infrastructures; further developing cybersecurity; cooperating on multinational projects, education, training exercises, and information exchange; reinforcing cooperation among national cyber defense stakeholders, and assessing its progress in meeting these goals (NATO, 2016a). Although there is no direct reference in the Pledge to issues of human rights or free access to the internet, the document is part of the broader scope of the Warsaw Summit, which paid considerable attention to human rights. The Warsaw Summit Communiqué (2016b) made nine separate references to human rights. These include indictments against Russia for its military build-up in Crimea and its abuses of the human rights of Crimean Tatars (2016b, § 17). Unlike the *Cyber Defence Pledge*, the Communiqué articulates that, together with benefitting from the latest cutting-edge technologies, NATO's Cyber Defense strategy will act in accordance with international law, including the UN Charter, international humanitarian law, and human rights law(2016b, § 70).

The declaration of a more recent meeting between the US and its NATO allies attests to another side to the issues of human rights and internet freedom. The first article of the Declaration posits NATO as a staunch defender of human rights, and argues:

> We are determined to protect and defend our indivisible security, our freedom, and our common values, including individual liberty, human rights, democracy, and the rule of law. NATO remains the foundation for strong collective defense and the essential transatlantic forum for security consultations and decisions among Allies. The Alliance will continue to pursue a 360-degree approach to security (NATO, 2018, § 1).

The Declaration decries Russia's human rights abuses against the Crimean Tatars and other neighboring communities and calls for an end to these activities. In a related manner, it urges Russia to reverse its recognition of Abkhazia and South Ossetia, thereby upholding the territorial integrity of Georgia (NATO 2018, § 7). Thus, early on in the document, NATO is posited as a defender of democracy and human rights while Russia is depicted as a major abuser. The Declaration stresses its commitment to defense against cyberattacks, yet "reaffirms its commitment to act in accordance with international law, including the UN Charter, international humanitarian law, and human rights law, as applicable (2018, § 20). The Declaration adds no qualifying statements to these goals, and thus reveals itself to be much more committed to human rights than the SCO, as evidenced by the *International Code of Cyber Security*. The Declaration, moreover, answers to the US aspiration for self-characterization, in this case, as Colin S. Gray stresses "[as product of] a discernible American strategic "culture," in both thought and behavior (1981, p. 22).

Separate from its activities with NATO, the US, together with some 31 other nations, is a member of the Freedom Online Coalition, an inter-governmental group, which is comprised of nations from the European Union; North America (Canada, Mexico); Central and South America (Argentina, Costa Rica); Asia (Japan, Mongolia, Georgia); Africa (Tunisia, Kenya, Ghana), and Oceania Australia, (New Zealand). Launched in 2011 at a conference held under the auspices of the Dutch government, it is dedicated to the protection and enjoyment of human rights on the internet. The overarching mission of the Coalition is to assure that "the human rights that people have offline [be] protected online (Freedom Online Coalition, 2021, The Coalition has issued a joint statement which, to date, is arguably the most thorough discussion of the relationship between human rights and cybersecurity. The joint statement asserts:

> […] a secure internet is central to the respect for human rights in the digital context. Cybersecurity measures should reinforce the availability, integrity, and confidentiality

> of information. These are essential to the security of the individual, especially in the digital context where physical security and digital information can be linked. Individuals cannot exercise their human rights if they do not have the security to do so. It therefore follows that cybersecurity and human rights are complementary, mutually reinforcing, and interdependent (Freedom Online Coalition, 2020a).

The Freedom Online Coalition stresses that it is essential for governments to incorporate the perspectives of all stakeholders from industry, the technology sector, civil society, and the academic community at the earliest possible stage into the development of a national cybersecurity policy., for "the private sector also plays a critical role in creating and maintaining digital services and infrastructure as well as introducing innovative initiatives promoting cybersecurity leadership" (2020a). The Coalition expresses its deep concern that some States assert "excessive control over the Internet under the pretense of ensuring national security while disregarding international human rights law and the principles of an open, free, secure, interoperable and reliable Internet (2020a). It further conveys its alarm that some States "have manipulated or suppressed online expression in violation of international law, including through discriminatory or politically motivated Internet censorship or Internet shutdowns, unlawful or arbitrary monitoring, and the arrest and intimidation of online activists for exercising their human rights" (2020a).

Also in 2020, the Freedom Online Coalition issued a joint statement on artificial intelligence and human rights. It stresses:

> When developed and used in full respect of human rights, AI [artificial intelligence] systems can complement human endeavors across fields such as public and precision health and environmental science to improve people's lives and support the UN

> Sustainable Development Goals. States play a critical role in promoting these benefits for all. (Freedom Online Forum, 2020b).

Nonetheless, the Coalition articulates concern that AI or diverse forms of remote biometric identification (RBI) can be used in the repression of individuals or communities, such as religious groups. Such a stance is, by implication, inimical to Russia's agenda—as well as to those of other members of the SGO—in that it may well be harmful to the "spiritual, moral, and cultural values of the State." The strategic cultures of Russia and the US, in this case, lie in direct opposition to each other in what concerns ideas shaped by history and experience.

Impasses for Russia and the US in the Development of a Counter Cyberterrorism Regime: Recent History

On a surface level, but one which is, nonetheless, extremely revealing, is the distrust that has developed between Russia and the US over recent events, both cyber and otherwise. Accusations of Russia's meddling in the US elections of both 2016 and 2020 have fueled deep mistrust of Russia in the US. This mistrust is evidenced both in the political sector and among the populace at large. Russia is perceived as a cyber aggressor due to accusations of its cyber attacks on Estonia, Ukraine, and Georgia. Of particular consequence is that, while one of these three countries is a member of the EU, the other two are westward looking. Russia's strategy has been to attempt to weaken Georgia by recognizing and supporting the break-away regions of Abkhazia and South Ossetia. In the case of the former, it can use the cultural and linguistic complexity of its own North Caucasus region to its advantage. The Ossetian language and culture is predominant in the Russia district of North Ossetia, and there are a great deal of affinities between the Ossetians living within the confines of the Russian Federation and their neighbors to the South. In a slightly more complex manner, the Abkhazians are related to the divergent Circassian populations of southern Russia, despite a difference in religion, most Circassians being Muslim.[20] Russia's support for the self-declared Donetsk People's Republic and Luhansk People's Republic and its annexation of Crimea have cause anxiety over the status of the town of Narva, a Russian-speaking enclave on Estonia's border with Russia (Josh Rubin 2019). Russia, in recent years, has clearly been asserting its authoritative and nationalistic character that has formed over the course of centuries of experience. What appears to be in evidence here is Russia's culture of elites, who "are socialized into a distinctive mode of thought" (Jack L. Snyder, 1977, p. 66). Russia's behavior has been consistently in tandem with its unique belief system.

Snowden's actions were actually perceived with mild acceptance by Russia. Although the affair led to a high level of tension between the US and its closest allies, Putin offered a mild scolding, agreeing that American surveillance had become "too intrusive," all the while praising Russia's intelligence services that operate within the confines of the law (*Putin Says Snowden Was Wrong to Leak Secrets. But Is No Traitor*, 2017). Putin's mixed reaction to Snowden's whistleblowing signaled somewhat better relations between Moscow and the new Trump administration. In 2020, while world leaders decried an attack allegedly instigated by Moscow on opposition leader Alexey Navalny, Trump's reaction was quite understated. Of course, the news hit during the controversy as to whether Moscow was allegedly once again interfering with the US elections, spreading allegations of voter fraud to the American people, Regarding the current situation between Moscow's relationship with Washington in the wake of Biden's recent name-calling, Susan B. Glasser claims that Russia is low on the US president's current agenda, given pressing domestic issues. The election of Biden marked a low moment in Russia-US relations, and the tide could turn in virtually any direction. Given the pandemic and vaccine roll-out, it is doubtful that the formation of a counter cyberterrorism regime with Russia will be a major priority in the near future.

Impasses for Russia and the US in the Development of a Counter Cyberterrorism Regime: Ideological Concerns

From an ideological perspective, the two aforementioned articles in Andrew Korunov and Olga Oliker's edited volume on US-Russian relations that deal with the perspectives of each country on cybersecurity issues triangulate closely with the foregoing analyses in this chapter. The cover of the edited volume is especially evocative. It depicts an eagle and a bear who stand on a road, intensely studying a map. A bilingual road sign indicates "danger" in whichever direction they choose. James A. Lewis offers a US perspective on the issue, and argues that, while Russia and the US have managed to cooperate successfully in initiatives related to counterterrorism, the addition of the term "cyber" has been problematic. Cybersecurity involves issues of freedom of expression of viewpoints, and Russia, together with other like-minded nations, prefer to use the term "information security" to emphasize the dangers that could be implicit in open access (James A Lewis, 2017, p. 63).

Lewis further stresses that another significant issue separating the positions of Russia and the US involves the positions of both States to the *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (2015b), which was made by the authors of the *Tallinn Manual*. Obviously, inasmuch as the US championed the authorship of the *Manual*, it was in full agreement with its discussions of the application of the concept of sovereignty of international law to cyberspace. Russia, on the other hand, took exception not only to this section, but also to the *Manual*'s discussion of the use of cyberattacks in warfare. Russia deemed that a cyberattack should be treated in the same way as an attack by a weapon of mass destruction (since the possibility of catastrophic damage is indeed there, and not as a permissible tool in warfare (James A. Lewis, 2017, p. 63. The US, moreover, feels that Russia deems NATO's cyber doctrine to be destabilizing and that this doctrine could sanction preemptive attacks.

Given that both the US and Russia have used cyberattacks for coercive purposes, the issue becomes more complex. What is likely at play here is that, even though both nations have engaged in similar behavior, their underlying motivations are very different, inasmuch as both seek to maintain the status quo of the ideational stance. It is necessary for both nations to come together to counter cyberterrorism in a way that accommodates the political interests of both countries.

A Russian perspective to the cybersecurity debate is provided in Koruov and Oliker's report by Pavel Sharikov (2017). In full recognition of the differences between Russia and the US in this field, Sharikov stresses that the fragmentation of the Internet "through which the internet is becoming both less global and less unified, and the intention of some governments to build a "national internet," complicates efforts to find common grounds in cyberspace" (2017, p. 69). Nonetheless, he reminds readers that Russia was an advocate for an idea brought forth by the Internet Corporation for Assigned Names and Numbers (ICANN), which was championed by the US Department of Commerce, that prescribed a multi-stakeholder system of Internet governance (Sharikov, 2017, p. 69). Sharikov emphasizes that when Russia proposed the creation of an international body under the auspices of the UN which would replace ICANN as the responsible entity for internet security, the US opposed the proposal, and President Obama transferred the efforts to this effect from ICANN to another international organization (2017, pp. 69-70).Sharikov discusses recent official Russian measures which essentially blocked access to clouds and allowed internet service providers to gather data on customers, store it for six months, and provide it to intelligence, if necessary. He argues that, although such measures may make a country less competitive economically, they were necessary for increasing Internet security (2017, p. 70). Sharikov acknowledges that these measures can indeed reduce the confidence of a potential cybersecurity partner, yet he stresses that the US has attempted to take similar precautions. An example cited by Sharikov is the

US's request that Apple provide iPhone data to the FBI in the wake of the San Bernadino shootings of 2015. Sharikov summarizes he challenges to regime formation as follows:

> Given the degree of internet fragmentation that has taken place to date and the acceleration of this process, any further international cybersecurity regime will be based on the various national regulatory regimes that are developed in accordance with each nation's particular political, legal, economic, and social context. It is clear that cyberspace is unique in that national governments cannot regulate it in the same way as other more tangible policy areas. Within this context, a key issue will be determining (or agreeing on) a proper balance between government and freedom of information (2017, p. 70)

In sum, the stalemate that has resulted from any attempt between Russia and the US to Form a counter cyberterrorism regime, or any cybersecurity regime, for that matter, is the result of a complex combination of both countries' historical perspectives, ideology, and reactions to recent events. This combination of factors is precisely that envisioned by Alastair Iain Johnston, who notes how states refrain from behavior that "threatens their immediate survival" (1995a, p. 35). The factors causing the impact cannot be simplified, nor can they be dealt with in isolation. One must view the US as a nation with a considerable sense of entitlement, whose 19th-century expansion was the logical outcome of a firm belief in manifest destiny, Its relationship to its neighbors and the people whose lands it appropriate, albeit no less expansionistic than Russia's context, were philosophically distinct, and pointed to two highly differentiated national psyches. Each country developed its own political strategies, yet in both cases, these bear witness to their shared need to demonstrate to the world, and to each other, their superpower status. There have, moreover, been high profile events that have tarnished their respective reputations internationally and that have led to a mutual sense of mistrust. Nevertheless, there is one faint ray of hope. The common threads of so many of their differences have been and will continue to be their opposing stance on freedom of speech and access to information and their contrary views on human rights. One can only hope that the two nations can agree to disagree on these two significant issues and work together towards a creation of a counter cyberterrorism regime that will benefit each of them as well as the global community.

CONCLUSION

A REACH FOR CONSENSUS THROUGH TRACK ONE-AND-A-HALF AND TRACK-TWO DIPLOMACIES

The intentions of Russia and the US to develop a regime to counter cyberterrorism have resulted in an impasse. As demonstrated in Chapter V, the primary impediments are located in two closely related arenas: human rights and freedom, and the ability to express and access information. For Russia, these concepts evoke Western ideas inimical to its own sense of security, both domestic and international. For the US, they imply freedoms essential to democracy and an open society. Granted, each nation could benefit greatly from cooperation to this effect, and moreover, a Russia/US counter cyberterrorism regime could have an enormously powerful impact on the security of other nations as well. The stalemate is serving to worsen the state of both international cybersecurity and counter terrorism in a broad sense. Official channels appear blocked, this due not only to the overarching political philosophies of each nation, but also to the historical relations between each country and the other’s bloc of allies. The positive energy and synergy of the 2006 edition of the workshop held jointly by the US National Research Council of the National Academies and the Russian Academy of Science. The presentations made by the Russian/US Working Group on Cyberterrorism Issues revealed a true potential for cooperation on a non-political level. The path to future cooperation was thus being paved as early as 2006, although it failed to involve official diplomacy. The Working Group constituted a promising example of Track Two Diplomacy (T2) and consisted of a forum in which Russians and Americans could come to understand the others’ perspective. Given a stalemate at the official level, T2 is decidedly the best option for fostering regime formation between the two nations in counter cyberterrorism.

Some Words on Track One-and-a-Half and Track-and Track Two Diplomacies

In a recent discussion of the role of non-official mediation, Tobias Böhmelt defines the phenomenon of multiple tracks of diplomacy as "initiatives by outside state or non-state parties to transform a dispute by communicating information, proposing new solutions, and directly influencing the crisis using carrots and sticks that can help generate movement towards potentially overlapping bargaining positions" (2010, p. 167). Böhmelt separates the closely related phenomena of Track Two Diplomacy (T2) and Track One-and-a-Half Diplomacy (T1.5), emphasizing that while T2 "encompasses unofficial, informal interaction between members of adversarial groups or nations," T1.5 "comprises public or private interaction between official representatives of conflicting actors mediated by a third party not representing a political institution" (2010, p. 167). He further clarifies his terms by emphasizing that Track One Diplomacy (T1) is "an inter-state process where communication goes from one official party directly to the decision-making apparatus of another actor" (2010, p. 168). As examples of T1, Böhmelt mentions the UN intervention during the crisis with Iraq in 1991 and the role of the United Kingdom's Lord Carrington during the Rhodesia-Zimbabwe independence process. What is at stake in T1 is the "authority and power of an official entity. The skills, resources and interests from these 'principals' directly influence the performance of T1" (2010, p. 168). In contrast, T2 involves "the informal interaction between members of adversarial groups or nations with the goal of developing strategies, influencing public opinions and organizing resources in ways that might help resolve the conflict" (2010, p. 168). T2 actors may be members of NGOs or grassroots groups, or they may be regional or local leaders. Böhmelt exemplifies T2 efforts with the international campaigns against South African apartheid and the work of Harvard professor Roger Fisher in El Salvador. According to Böhmelt, "T2 can be more subtle, personal and free from the constraints of 1, as it involves NGO activity and back-channel measures" (2010, p. 168).[21] Böhmelt points out that both Diana

Chigas (2004), and Joseph V. Montville (1991) have argued that "value-based conflicts about identity, survival and fears of the other can only be effectively addressed by T2 diplomacy that seeks to change the underlying relationships so as to promote a mutual understanding and acknowledgement of each other's concerns" (Tobias Böhmelt, 2010, p. 168).

Böhmelt finds considerable potential in T1.5, which he identifies as having come about as a response to situations in which "official actors have no incentives to engage in a conflict and/or T2 efforts show no effect at the grassroots level […] T1.5 is a public or private interaction between official representatives of disputants that is mediated by a third party not representing a political institution" (2010, pp. 168-169). He explains that T1.5 can be undertaken by such individuals as former US president Jimmy Carter, prominent academics, or even religious leaders. Specific examples of T1.5 efforts include the Oslo Peace Process, Sant'Egidio's negotiations in the conflict in Mozambique, and the Guinea Worm Ceasefire mediated by the Carter Center. For Böhmelt, T1.5 can combine the best aspects of T1 and T2. Yet it can also suffer from the weaknesses of both.

In any case, Böhmelt finds both T1.5 and T2 less coercive than T1. Rather than exercising power, they can foster support for agreements at the local level. Their effectiveness lies in their ability to convince actors, appeal to their common understanding, and establish a peaceful settlement through private discussions" (Böhmelt 2010, p. 170). T1.5 diplomacy is effective in part by its "developing and maintaining a wide network of contacts, able to spread respect and trust among the disputing parties" and by "providing a neutral, low-key, safe and non-judgmental environment, such as in workshops or reconciliation programs to facilitate interaction" (2010, p. 170). Böhmelt stresses:

> These circumstances can make participants freer to share fears and explore ideas for resolution, free from the constraints of government positions in a non-binding and flexible way. In this sense, T2 is a form of what Kydd & Snidal (1997: 123-124)

> characterize as 'cheap talk' strategies that can convey information about the range of mutually acceptable agreements and sustain coordination. Afterwards, parties discuss ways to end a conflict, but 'can walk away from them without penalty'. More generally, T2 interventions can bring antagonists closer to a peaceful settlement without committing the parties too early to a binding agreement. This track mainly relies on communication facilitation (2010, p. 170).

Of particular consequence is that T1.5 and T2 are normally employed in the context of actual conflicts. Nonetheless, especially as evidenced by the auspicious beginnings brought about by the Russian/US Working Group on Cyberterrorism Issues, it becomes evident that similar approaches are likely to be fruitful in the case of regime formation. What is at stake is the building of trust, and tactics lying outside of the confines of official diplomacy are more likely to be unencumbered by the confines of official policies and state agendas.

The Need for Building Trust

Russia and the US lack mutual trust, and their misgivings play out on ideological, cultural, and historical levels. As mentioned in Chapter IV, the US has never suffered invasion or wars on its turf as has Russia. Moreover, it has never had the same tumultuous relationships with its neighbor that Russia has suffered for centuries. Although both countries can be deemed expansionist, they are expansionist for totally different reasons. While Russia seeks self-preservation, the US feels the entitlement of manifest destiny. During the Cold War, the ideological rift between Communism and the market economy was a driving force in the international divide commanded by the two superpowers. Upon the collapse of Communism, one would have expected the divide to have been drastically reversed. Yet Russia’s history had led to its acceptance of authoritarianism and its wariness of democracy. As Ivan V. Radikow asserts, Russia’s political system is hybrid, a blend of democratic institutions and autocratic governing methods (2019, p. 33). He argues that, given the conditions of "unconsolidated democratic culture of cooperation between the state and the society, the attitude of the majority of citizens to the contemporary political authorities in Russia is, to a high degree, based on trust in Vladimir Putin" (2019, p. 33). Extending Radikow's discussions of trust in government among citizens to the broader level of political structure, one can argue that the cult of personality embodied by Putin reinforces the authoritarian nature of the Russian state.

When it comes to cyber issues, both countries have reason to distrust the other. The US has found extensive evidence to indict Russia for interference in its 2016 and 2020 elections. (Kim Young Mie, 2020). Reciprocally, the world has been enlightened to the US's extensive use of cyberespionage by virtue of the Snowden affair. And to add to the equation, the transition between the Trump and Biden governments has been especially trying for Russia/US relations (James Goldgeier, 2021). It is essential to further stress that this distrust, particularly in the US, is evident not only in branches of the government, but also in public opinion (Lydia Saad, 2019). In any case, the crowning bone of contention is the two nations' opposing views on issues related to human rights and freedoms of speech/information. In sum, trust must be built from the bottom up in order for regime formation to be a possibility.

Jonah Force Hill maintains that countries such as Russia and China have argued that the organization and processes that have led to the standardization of the internet are both "outmoded and inequitable." He stresses that:

> [Russia and China] contend that the current process unfairly favors American firms; that it produces standards with insufficient built-in security; and that it leads to standards that allow for a degree of freedom fundamentally at odds with the social norms of some nonwestern nations. As a result of these concerns, the technical design decisions that were historically the sole province of engineers and academics have

> increasingly come under the political pressures of governments seeking to influence and reform them (2012, p. 50).

The eventuality of trust in cyberspace, thus presents a complex set of challenges.

Catherine Lotrionte and Tim Maurer (2012) affirm that the Internet is no longer merely a tool for academics or a tool through which to build a new economy. Rather, it is tied today to the politics of national and international security (2021, p. 3). Lotrionte and Maurer explain that, in the early days of the Internet, those who invented the tool and those who used it consisted of a small group of academics and computer scientists, and comprised a pocket-sized community where everybody knew each other (2012, p. 4). Today, the one billion users of the Internet are spread throughout the world, mostly in wealthy Western countries. Nonetheless, the Internet is rapidly spreading through developing countries and is host to a wide diversity of cultures and value systems. The need to build trust in cyberspace is growing just as rapidly (2010, p. 4).

From a Russian perspective, Anatoly Streltsov compares confidence-building strategies between nations in cyberspace to such measures between militaries in that they "[…] neutralize the cyber threats of opposing states in peacetime and wartime, prevent and resolves crises in the area of information infrastructure, combat cybercrime and information terrorism, and promote states' national cultural values and political preferences in foreign countries." (2012, p. 25). Streltsov stresses the importance of talks held at the UN, including those initiated by the International Group of Governmental Experts as well as those held at international conferences. According to Streltsov, these talks have been important in that "they have allowed the international community to develop the political capital required to reduce the danger posed by the malicious use of information and communications technologies, criminal organizations, and individuals" (2012, p. 26). Streltsov makes his way through a number of agreements that suggest possibilities of relatively successful international agreements on cybersecurity, including those of the International Group of Government Experts, efforts by the Union State of Belarus and Russia, the Collective Security Treaty Organization (CSTV), and the World Summit on Information Security, among others.[22] He stresses the four areas of concern identified by the 65th Session of the UN General Assembly (2010-2011) (UN General Assembly 2010). These include 1) the fear that information and communications technologies can used as tools in warfare for political purposes and thereby disrupt the stable operation of the Internet; 2) concerns in the latent malicious functions in technologies; 3) the potential for an information arms race and the use of information weapons, and 4) the eventuality that the global information infrastructure can be used for subversive purposes. Stretskov emphasizes that the most favorable scenario can be attained "if confidence-building measures are developed to help states ensure human rights and freedoms, provide free and independent development of national communications, improve the well-being of citizens, and improve [the states'] cultural integrity and security (2012, p. 32). It is significant that Streltsov is Vice-Director of the Lomonosov Moscow State University's Information Security Institute. He has further served in the US as a Research Associate Professor at Dartmouth University and as a Research Physicist at the Naval Research Laboratory in Washington, DC. He has had research sponsored by NASA, the ONR (Office of Naval Research), the US Air Force, and the Defense Advanced Research Projects Agency.

Streltsov as a scholar has gained considerable recognition in both Russia and the US. His discussions of the future of cybersecurity are clearly taken from each national discourse. From the US perspective, he argues for the protection from human rights and freedoms, at the same time respecting Russian concerns for cultural integrity (2012, p. 32). The clout he holds with each government suggests the potential for T1.5 in that he could clearly mediate between official channels in Russia and the US. Clearly, he holds an in-depth understanding of both countries, their history, cultural values, and security strategies.

US/Russian Working Groups

It is necessary to return to the counterterrorism workshops jointly organized by the Russian Academy of Science and the US National Research Council of the National Academies, which were held in Washington, DC in 2002, 2004, and 2006. The most significant accomplishment of these workshops was the establishment of the Russian/US Working Group on Cyberterrorism. As discussed in Chapter IV, the Group was composed of Russian and American academics in such fields as public policy, corporate management and the hard sciences, as well as officials from the US National Research Council of the National Archives and the Russian Office for North American Scientific Cooperation. In the days the Group spent together visiting venues related to cybersecurity in the Washington, DC area, it is likely that a sense of camaraderie and joint purpose emerged. The heavy academic presence in the talented group of men and women, and their lack of direct involvement in official political processes most likely allowed them to put state agendas aside and see beyond impasses. Discussed in Chapter IV were the main outcomes reported at the Workshop by the Working Group. At the forefront of their statement were the need for cooperation between the two nations and related academic exchanges and education processes.

In March 2017, Svetana Lukash, a Russian official announced that presidents Vladimir Putin and Donald Trump had agreed to discuss issues of cyber security, either via the UB or in the context of a working group (*Moscow in Talks with US to Create Cybersecurity Working Group: RIA Report*, 2017). Officials in US and European intelligence stressed that they themselves were not participating in the talks, inasmuch as these were confined to mid-level politicians. One US official described the idea as a "pipe dream," given that Russia still denies having interfered in the 2016 US elections. Thomas Bossett, the leading counterterrorism adviser in the Trump government, argued that "it would be premature to suggest that the United State would be talking to Russia about a possible cybersecurity 'partnership'" (*Moscow in*

Talks with US to Create Cybersecurity Working Group: RIA Report, 2017). Bosset further stressed that Russia and the US had not reached a point of trust that would lead to such a partnership.

A more recent discussion by international security expert Emilio Iasiello looks back at the 2017 claims that such a working group would be started. He posits a slightly different viewpoint from Bossett, arguing that the establishment of a working group could be a forum in which mutual trust could slowly be developed. Iasiello feels that such a group could both initiate dialogue on issues that have to date stalemated in international fora, among these the cyber norms of state behavior and Internet governance and work collaborative on cyber problems of concern to both countries, including cybercrime and cyberterrorism (Emilio Iasiello, 2020). Although the notion of a working group between Russia and the US may well be "ludicrous," Iasiello concludes:

> […] given the realities of cyber space and the fact that no state has a great handle on securing its overall cyber security posture, including critical infrastructures, having discussions about where the two can come together to address problems doesn't seem so silly. It seems sillier not to give it a try (Emilio Iasiello, 2020).

There remains no doubt that the lack of trust between Russia and the US, a situation that has worsened considerably in recent months, is one of the primary impediments to the establishment of a counter cyberterrorism regime between the two countries.[23] Yet Iasiello may not be overly optimistic in his suggestion that a working group could foster trust over time. The initial efforts of the Russian/US Working Group on Cyberterrorism were most promising, yet for reasons unclear, the group fizzled when the bi-national workshop failed to convene after 2006. The fact that the Workshop disappeared from sight at the time of the global financial crisis may well suggest that funding issues may have played a substantial role in its demise. What was especially auspicious in the case of the Working Group was the personal interaction among its participants. Moving forward some 15 years, one must note that Academia and NGOs, have learned an important lesson from the ongoing pandemic, they can practice their craft, albeit in a less personal venue, through the use of virtual environments. It is time to bring together a group of Russian and American academics, who are open to each other's perspectives and unmotivated by official agendas, to take up the challenge of the former Russian/US Working Group on Cyberterrorism. There may be other individuals such as natoly Stretsov, who have worked and gained recognition on both sides of the divide, and there are decidedly a good number of young academics who would be willing to work to combat cyberterrorism on a global level. These individuals could doubtless form a dynamic Working Group, regardless of whether or not one is formed on an official level. T2 or T1.5 both could provide excellent options. The constitution of the working group and the level of connectedness of its individuals to official channels would determine which of the two is likely to constitute the most auspicious strategy. Russia and the US are indeed at odds, in their ideologies, their competition to maintain or regain superpower status, and their respective historical heritage. Yet now is the time for a joint group of specialists to forge ahead in the fight against cyberterrorism. One can conclude by rethinking Margaret Mead's hackneyed and possibly apocryphal quote,[24] and perhaps breath into it some new life through lexical and grammatical changes. "Never doubt that a small joint group of concerned experts can change the field of cybersecurity. It's the only thing that ever can."

ENDNOTES

[1] For an extensive discussion of the history of the Baader-Mainhof gang, see Stefan Aust (2009), *Baader-Mainhoff: The Inside Story of the R.A.F*.

[2] An up-to-date collection of essays on ETA edited by Rafael Leonisio, Fernando Molina, and Diego Muro (eds.) (2016) reaches beyond the mere interest of terrorism and looks at well at recent processes of democratization.

[3] The Russian brain drain and its aftermath are explored by Andrei V. Korobkov and Zhanna A. Zaionchkovskaya (2012).

[4] One is reminded here of a quip by Ayn Rand, a Soviet émigré to the US, who developed the critical framework of philosophical objectivism and whose name is associated with the libertarian movement in the US. Rand asserts: "There can be no compromise between a property owner and a burglar; offering the burglar a single teaspoon of one's silverware would not be a compromise, but a total surrender—the recognition of his right to one's property" (93). Such a remark characterizes the US reluctance to reach any level of compromise with Russia.

[5] For a study of the financing mechanisms of terrorist organizations, see Michael Freeman and Moyara Ruehsen (2013).

[6] Although Maura Conway (2003) cites Pollitt as the author of this definition, she fails to provide an exact source or date for his remarks (p. 35).

[7] Some words are in order regarding general concepts of regime building which, although following outside of the primary discussion of this thesis, are nonetheless significant to the broader context of counter cyberterrorism regimes.

Tim Stevens (2017)) discusses the three domains in which a global governance architecture is emerging—cyberwarfare, cybercrime, and export controls. He argues that the best way in which to control cyberweapons is through regulation, and not an outright ban. For Stevens, a governance regime for cyberweapons "is developing quietly and haltingly. It is fragmented and contested but perhaps more constructive than none at all."

In an expanded version of his study, Stevens (3028) focuses on the non-existence of a global governance regime to oversee the issue of cyberweapons. He draws upon a power-analytical approach to identify four areas that work together to constrain the formation of such a regime. First, the NATO Cooperative Cyber Defense Center of Excellence (CCD COE) was established in 2008 in Tallinn, Estonia, and provides assistance to NATO states on issues of cybersecurity. This initiative resulted in the publication of the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Schmitt 2017). Written from a US/NATO perspective, the *Manual* deepens disagreements between the West and its adversaries. Second, Steven analyses structural power and the cyberweapons market, and foregrounds the role of the US in such a market. Third, Stevens looks at the very structure of the internet, and how it, by nature, supports U.S. issues. Finally, he examines how issues of state sovereignty are affected by the formation of such a regime.

Exploring academic discourse on the nature of security regimes, Hynek argues for epistemological pluralism, yet one which is grounded in a study of the operations of power, including productive power. Although not specifically addressing the issue of cybersecurity, Hynek proposes a model which can apply to this ``domain, particularly in what concerns the use of diverse theoretical models, all the while framed by the overarching analysis of power. Vitek Střítecky and Nik Hynek (2018), follow suit with the epistemological processes of Hynek's aforementioned study. In a synthesis of the power-analytical approach to global security regimes, they argue that existing prohibition/regulatory systems fall into three clusters: humanitarian (e.g., small arms, anti-personnel landmines), weapons of mass destruction, and unconventional (e.g., drugs and cyberweapons). They study these from the perspective of productive power; contingent systems of differentiation; real/imagined military/security centrality, and manipulation of categories. The combination of these categories allows for a robust study, allowing the most prominent features of very divergent cases to come to light.

Bringing the issue of regime building to a regional level, Yamin Tughral argues that through the development of a mutually-agreed-upon cyberspace regime, regional groups can cooperate with each other to fight cyberterrorism, He suggests that such cooperation be developed incrementally, starting with less sensitive domains such as universities and other academic institutions, dismissing, in the early stages of cooperation, areas related to national security. Such initial cooperation can become both intra bloc and inter bloc and form the basis of an international program to identify common threats. It can counter these through the monitoring and tracking of non-state actors who use cyberspace for recruitment, propaganda, financing, and planning of terrorist attacks. The cooperation can be extended to other domains once confidence is built among the nations involved.

[8] Having had early roots in the pragmatism of John Dewey, who recognized the importance of a combination of cultural factors and personal experience in the formation of the individual (John Dewey, 1938), it made its way into diverse realms of the social sciences. In the 1970s, Lev Vygotsky's meditations on the nature of language and social interaction were of special importance. Although often not deemed a social constructivist due to his overarching devotion

to Marxism and forays into liberation theology, Paulo Freire, nonetheless, reflected the potential of social constructivism as a framework for explaining the role of social interaction in the learning process.

[9] For a discussion of the broader concepts of Internet governance, see Carol M. Glen, 2017.

[10] In 2017, India and Pakistan both became members. Bahrain and Qatar have officially applied for membership. Mongolia, Afghanistan, Iran, and Belarus are observer states. Dialogue partners include Armenia, Azerbaijan, Nepal, Sri Lanka, and Turkey. Armenia, Azerbaijan, Bangladesh, East Timor, Nepal, Sri Lanka, Egypt, and Syria have applied for observer status. Israel, Maldives, Ukraine, Iraq, and Saudi Arabia have applied to be dialogue partners. By virtue of a resolution by the UN National Assembly, Turkmenistan has officially been recognized as a neutral country, and hence, its membership in the organization is rendered impossible.

It is significant to note that a number of inimical nations are involved in the Organization or have applied to participate therewith (Ukraine/Russia; Israel/Syria' Armenia/Turley; Armenia/Azerbaijan, India/Pakistan).

[11] The *Tallinn Manual* refrains from making any specific accusation of Russia in the Estonia and Georgia attacks.

[12] For a detailed analysis of 1950s cultural exchanges between the US and the Soviet Union, see Helen B. Shaffer (2001), "Cultural Exchanges with the Soviet Union," *CQ Researcher*.

[13] The BCC did not meet in 2020 due to COVID 19 (US Department of State 2021).

[14] In an earlier edition of the *New York Times* of 26 March, 2014, it was erroneously published that Russia had annexed all of Ukraine, not just Crimea (Allison Smale and Michael D. Shear, 2014).

[15] It is necessary to recall that, while the US has a highly politically-active Armenian diaspora, which led to the exclusion of Azerbaijan from US aid to support democracy in the new countries of the Commonwealth of Independent States, while Turkey is closely aligned with Azerbaijan, another Turkic Muslim country. For a detailed chronicle of the development of the conflict between Armenia and Azerbaijan, see Elgün Karimov (2009), "Jockeying for Power in the South Caucasus: The Interests of Russia and the U.S. in the Nagorno-Garabagh Conflict"

[16] One can contrast Russia's slow move to power with the 19th-century image of Russia's great rush forward presented by Nikolai Gogol in *Dead Souls* (1842). For an analysis of this metaphor, see Judith Deutsch (1987).

[17] For an in-depth study of manifest destiny, see Robert Miller (2006). Also, an especially eludating analysis of manifest destiny in American history and culture can be found in Annette Kolodny (1984). Kolodny posits US expansionism in sexual terms, and hence her work is titled *The Lay of the Land*.

[18] The letters list China the Russian Federation, Tajikistan, and Uzbekistan as signers, but both also include the signatures of representatives from Kazakhstan and Kyrgyzstan.

[19] On a regional level, a nation that has expressed concern over the Code is Mongolia. See Gallbaater Lkhagvasuren (2017).

[20] It is noteworthy to mention the work of George Hewitt, Professor Emeritus of the University of London and specialist in Caucasian languages and regional studies, who became Great Britain's honorary ambassador to Abkhazia. For more about Abkhazia's neighbors to the North, see Kadir I. Natho, *Circassian History*. a work useful in sorting out the complex cultural entanglements of the region.

[21] Böhmelt refers the reader, in this context, to the work of such scholars as Cynthia Chataway and Andrew Kydd.

[22] For more information on the World Summit on the Information Society, see United Nations Department of Economic and Social Affairs, Sustainable Development (2021).

[23] A ray of hope in relations between Russia and the US is the recent news that President Biden has become the first present in US history to recognize the Armenian Genocide (1915-1917) as a genocide as opposed to a massacre (Mahmadi, Aamer, Mathew Lee. And Zeynep Bilginsoy (2021). Former administrations had declined to do so. There hesitance involved the inevitable condemnation by Turkey, the US's second-closest ally in the Middle East. Despite Turkey's furor over Biden's 24 April 2021 announcement, Russia may react differently. After all, Armenia is its closet ally in the strife-ridden South Caucasus, and moreover, the two nations are united by the Eastern Orthodox faith.

[24] Margaret Mead's famous quote, "Never doubt that a small group of concerned citizens can change the world. It's the only thing that ever has," is a widely-known observation that does not appear in the anthropologist's known work. An early use of it was as an epithet to Chapter

VI, “The Politics of Consciousness” in Donald Keys’s *Earth to Omega: Passage to Planetiztion* (1982, p. 79).

BIBLIOGRAPHY

Absatarov, R.R. (2018), “Protivodyeistviye komptuteromu terrorizmu,” *Proceedings of the Sixth Penxa Conference on Science and Practice*, Penza, Russia: International Center for Science and Practice, pp. 172-174.

Adamsky, Dina P. (2008), *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel*, Palo Alto: Stanford University Press.

Arms Control Association (2019), “The Intermediate-Range Nuclear Forces (INF) Treaty at a Glance,” https://www.armscontrol.org/factsheets/INFtreaty, (Accessed 1 March, 2021).

Aris, Stephen (2009), “The Shanghai Cooperation Organisation: ‘Tackling the Three Evils’. A Regional Response to Non-traditional Security Challenges or an Anti-Western Bloc?” *Europe-Asia Studies* 61.3, pp. 457-482.

Arms Control Association (2020), “The Anti-Ballistic Missile (ABM) Treaty at a Glance,” https://www.armscontrol.org/factsheets/abmtreaty, (Accessed 1 March, 2021).

Atnushev, Vadim R. and Sadaf N. Yakheeva "Myezhdunarodnoye sotrudichestvo v borb'ye s kiberprestupnosct'ku I kiberterrorismom/International Cooperation on Cybercrime and Cyberterrorism," *Yevraiishaya integratsiya: ekonomika, pravo politika* 3: pp. 37-42.

Aust, Stefan (2009), *Baader-Mainhoff: The Inside Story of the R.A.F.*, Cambridge: Cambridge University Press.

Bagge, David (1999), *Unmasking Maskirovka: Russia's Cyber Influence Operations*, New York: Defense.

Baram, Gil and Harel Menashri (2019), "Why Can't We Be Friends? Challenges to International Cyberwarfare Cooperation Efforts and the Way Ahead," *Contemporary Strategy* 30:2, pp. 89-97.

Batchelor, Tom (2017), "Russia Announces Plan to Formally Leave G8 Group of Industrialized Nations after Suspension for Crimea Annexation," *The Independent* 13 January 2017, https://www.independent.co.uk/news/world/politics/russia-g8-kremlin-crimea-ukraine-vladimir-putin-g7-g20-a7525836.html, (Accessed 22 March, 2021).

BBC News (2018), "Russia Meddled in All Big Social Media arpimd U.S. Elections," 17 December, https://www.bbc.com/news/technology-46590890, (Accessed 2 April, 2021).

Belli, Luca (2019), "From BRICS to CyberBRICS: New Cybersecurity Cooperation," *China Today* 13 November, http://www.chinatoday.com.cn/ctenglish/2018/tpxw/201911/t20191113_800184922.html, (Accessed 12 September 2020).

Bing, Christopher, Joseph Menn, and Raphael Satter (2021), "Putin Likely Directed 2020 U.S. Election Meddling, U.S. Intelligence Finds," *Reuters* 16 March, https://www.reuters.com/article/usa-election-cyber-int/putin-likely-directed-2020-u-s-election-meddling-u-s-intelligence-finds-idUSKBN2B82PF, (Accessed 22 March, 2021).

Bekki, Luca (2021), *CyberBRICS: Cybersecurity Regulations in the BRICS Countries*, Cham: Switzerland: Springer.

Blatter, Joachim and Till Blume (2008), "In Search of Co-Variance, Causal Mechanisms or Congruence? Towards a Plural Understanding of Case Studies," *Swiss Political Science Review* 14:2, pp. 315-356.

Böhmelt, Tobias (2010), "The Effectiveness of Tracks of Diplomacy Strategies in Third-Party Interventions," *Journal pf Peace Research* 47.2, pp. 167-178.

Bozeman, Adda B. (1976), "War and the Clash of Ideas," *Orbis* 20.1, pp. 61-102.

.

Brenner, Susan W. (2006), "Cybercrime, Cyberterrorism and Cyberwarfare," *Revue International du droit penal* 3.77: pp. 453-471.

BRICS (2016), BRICS, BRICS Summit Goa Declaration, http://www.brics.utoronto.ca/docs/161016-goa.html, (Accessed 1 April 2021).

BRICS (2019), "The Declaration of the BRICS Communications Ministers Meeting held in Brasília, Brazil in August, 2019," http://www.brics.utoronto.ca/docs/190814-communications.html, (Accessed 4 April 2021).

Buck, David (2017), "The New Milledium Blues," *Tedium* 27 December, https://tedium.co/2017/12/27/y2k-pop-culture-oddities/ (Accesssed 2 August 2020).

Cassim, Fawzia (2012), "Addressing the Specre of Cyber Terrorism: A Comparative Perspective," *P.E.R.* 15.2., pp. 381-416.

Chataway, Cynthia (1998), "The Evolution of Diplomacy: Coordinating Tracls I and II," in Dorn, Walter, ed., *World Order for a New Millenium: Political, Cultural and Spiritual Approaches to Building Peace*, New York: Saint Martin's 139-146.

Chigas, Diana (2003), "Track II (Citizen) Diplomacy," in Burgess Guy and Heidi Burgess, eds. *Beyond Intractability*, Boulder: CO: Conflict Research Consortium, University of Colorado.

Choudhury, Dipanjan Roy (2020), "BRICS: Counter-terror strategy adopted at summit puts the onus on China,"

The Economic Times, https://economictimes.indiatimes.com/news/defence/brics-counter-terror-strategy-adopted-at-summit-puts-the-onus-on-china/articleshow/79289082.cms?from=mdr, (Accessed 31 March, 2021).

Choudhury, Dipanian Roy (2021), "Counter-terror strategy & multilateral reforms to top agenda

India's BRICS Presidency," *The Economic Times* 22 February, https://economictimes.indiatimes.com/news/defence/india-to-focus-on-counterterror-cooperation/articleshow/81144793.cms?from=mdr, (Accessed 8 April, 2021).

Clinton, William J. and Boris Yeltsin (1998). "Joint Statement on Common Security Challenges at the Threshold of the Twenty-First Century, "*Public Papers of the Presidents of the United States: William J. Clinton, 1998, Book II*, Washington, D.C,, US Government Printing Office, pp. 505-507.

Collin, Barry C. (1997*, Marcg*), "The Future of Cyberterrorism," *Crime and Justice International*, March, pp. 15-18.

Conway, Maura (2003), "Cyberterrorism: The Story So Far," *Journal of Information Warfare* 2.2, pp, 33-42.

Council of Europe (2001), *Convention on Cybercrime*, https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf, Accessed 4 March 2021.

Council of Europe Treaty Office (2021), *Chart of signatures and ratifications of Treaty 185—Convention on Cybercrime: Status as of 25/03/2021*, 25 March, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=EmvNwg*TW*, Accessed 25 March, 2021.

Council on Foreign Relations (2018), “Increasing International Cooperation in Cybersecurity and Adapting Cybernorms,” February 23, https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms, (Accessed 15 September, 2020).

CyberBRICS, (2021). *CyberBRICS https://cyberbrics.info/*, (Accessed 1 April, 2021).

Davidson, Mary Ann (2009), “The Monroe Doctrine in Cyberspace: Expansion of Remarks Made in Testmony Given to the Homeland Security Subcommittee on Emerging Threats, Cybersecurity and Science and Technology,” 10 March, https://act.nato.int/images/stories/events/2010/gc/ws_cyb_monroedoctrine.pdf¸(1 September, 2020).

Denning, Dorothy E. (1999), “Activism, Hactivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy,” in Arquilla, John and David Ronfeldt, eds., *Networks and Netwards: The Future of Terror, Crime and Militancy*, Santa Monica: RAND Corporation, pp. 239-288.

“Despite Campaign Vow, Obama Declines to Call Massacre of Armenians ‘Genocide’” (2019), *The New York Times* 22 April, https://www.nytimes.com/2016/04/23/world/europe/despite-campaign-vow-obama-declines-to-call-massacre-of-armenians-genocide.html?smid=tw-nytimesworld&smtyp=cur, (Accessed 24 April 2021).

Deutsch, John (1996), *Statement before the US Senate Governmental Affairs Committee (Permanent Subcommittee on Investigations)*, 25 June, http://www.nswc.navy.mil/ISSEC/Docs/Ref/InTheNews/fullciatext.html, (Accessed 30 May 2020).

Deutsch, Judith (1987), "Perspective from the Threshold: The Troika of *Dead Souls*," *Ulbandus Reviewe V*, pp. 3-17.

Dewey, Jon (1938), *Experience and Education*, New York: Macmillan.

Dogrul, Murat, Adil Aslan, Eyyup Celik (2011), "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism," in Czosseck, Christian, Enn Tyugum and Thomas Wingfield, eds., *3rd International Conflict on Cyber Conflict*, Tallinn: CCD COE.

Eitelhuber, Norbnert (2009), "The Russian Bear: Russian Strategic Culture and What It Implies for the West," *Connections* 9.1: pp. 1-28.

European Court of Human Rights (1950), *European Convention on Human Rights*, https://www.echr.coe.int/documents/convention_eng.pdf (Accessed 7 March 2021).

European Parliament, Directorate General for External Policies (2014), *Russia's G8 Presidency: With an Ambitious Agenda, Can Moscow Deliver?*, https://www.europarl.europa.eu/RegData/etudes/briefing_note/join/2014/522324/EXPO-AFET_SP(2014)522324.EN.pdf, (Accessed 31 March 2021.

Faleti, Yemi (2018), "Cyber Attacks in a Digital Age," Stevenson University Online, https://www.stevenson.edu/online/about-us/news/cyber-attacks-digital-age, (Accessed 29 July 2020).

Farrell, Theo (2002), “Constructivist Security Studies: Portrait of a Research Program,” *International Studies Review* 4.1, pp. 49-72.

Federal Bureau of Investigation (1999), *Project Megiddo*, https://www.oodaloop.com/wp-content/uploads/2013/10/projectmegiddo.pdf, (Accessed 20 July 2020).

Federal Trade Commission (2015), “Update on the Safe Harbor Framework” 25 July, https://www.ftc.gov/tips-advice/business-center/guidance/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor, (Accessed24 March, 2021.

Finnemore, Martha, and Kathryn Sikkink. (2001), “Taking Stock: The Constructivist Research Program in International Relations and Comparative Politics,” *Annual Review of Poitical Science* 4, pp. 391-416.

“France’s Hollande Speaks to Obama on US Spying Reports” (2013), *Al-Arabiya*, 22 October, https://english.alarabiya.net/News/world/2013/10/22/Hollande-expresses-disappointment-to-Obama-over-U-S-spying-, (Accessed 22 March, 2021).

Freedom Online Coalition (2020a), *Human Rights Impact of Cybersecurity Laws, Practices and Policies,* https://freedomonlinecoalition.com/wp-content/uploads/2020/02/FOC-Statement-on-Human-Rights-and-Cyber-Security-07.02.pdf, (Accessed 31 March, 2021).

Freedom Online (2020b) *FOC Joint Statement on Artificial Intelligence and Human Rights,* https://freedomonlinecoalition.com/news/foc-issues-joint-statement-on-artificial-intelligence-and-human-rights/, (Accessed 26 March 2021).

Freedom Online (2021), “About Us, https://freedomonlinecoalition.com/about-us/about/, (Accessed 22 March, 2021).

Freire, Paulo (1970), *The Pedagogy of the Oppressed*. New York: Herder and Herder.

Freeman, Michael and Moyara Ruehsen (2013), “Terrorism Financing Methods: An Overview,” *Perspectives on Terrorism* 17.4, pp. 5-26.

Gady, Franz-Stefan and Austin, Greg (2010). *Russia, the United States, and Cyber Diplomacy: Opening the Doors*, New York: EastWest Institute, https://www.files.ethz.ch/isn/121211/USRussiaCyber_WEB.pdf (Accessed 31 May 2020).

Gates, Gill (2001), “Shanghai Five: An Attempt to Counter U.S. Influence in Asia*?,” Brookings*, https://www.brookings.edu/opinions/shanghai-five-an-attempt-to-counter-u-s-influence-in-asia/, (Accessed 17 February 2021).

Gelb, Leslie H. (1985), “Three Past Presidents May Brief Ronald Reagan,” *The New York Times* 5 November ,https://www.nytimes.com/1985/11/05/world/three-past-presidents-may-brief-reagan.html (Accessed 13 March, 2021

George, Alexander L. (1967, *Operational Code: A Neglected Approach to the Study of Political Leadership and Decision Making—Memorandum*, Santa Monica, CA: The RAND Corporation.

Giles, Keir (2012), "Russia's Public Stance on Cyberspace Issues," in Czossek, Christian, Rain Ottis, and Katharina Ziolkowski, eds, *4thInternational Conference on Cyber Conflict, Proceedings*, Tallinn: NATO Cooperative Cyber Defense Centre of Excellence, pp. 63-76.

Glen, Carol M. (2017), *Controlling Cyberspace: The Politics of Internet Governance and Regulation*, Westport: CT: Praeger.

Goldgeier, James (2021), "U.S.-Russian Relations Will Only Get Worse," *Foreign Affairs* 6 April, https://www.foreignaffairs.com/articles/russia-fsu/2021-04-06/us-russian-relations-will-only-get-worse, (Accessed 22 April, 2021).

Gogol, Nikolai, D.J. Hogarth, trans. (2016) (originally published in 1842), https://www.gutenberg.org/files/1081/1081-h/1081-h.htm, (accessed 13 April, 2021).

Gray, Colin S. (1981), "National Style in Strategy: The American Example," *International Security* 6.2, 2, pp. 21-47.

Grigsby, Alex (2018), "The United Nations Doubles in Workload on Cyber Norms, and Not Everyone Is Pleased," Council on Foreign Relations, 15 November, https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased, (Accessed 21 September, 2020).

Growth in the Americas/América Crece (2019), *Growth in the Americas*, https://www.state.gov/wp-content/uploads/2019/11/America-Crece-FAQs-003-508.pdf, (Accessed 8 February 2021).

Harris, David (1997), “Ex-CIA Head Deutsch Warns of Electronic-Terrorism Challenge,” *Jerusalem Post*, 30 December, p. 1.

Hill, Jonah Force (2012), “A Balkanized Internet? The Uncertain Future of Global Internet Standards,” *Gerogetown Journal of International Affairs, Special Issue--International Engagement on Cyber 2012: Establishing Norms and Improving Security* (2012), pp. 49-58.

Huysmans, Jef (2002), “Defining Social Constructivism in Security Studies: The Normative Dilemma of Writing Security,” *Alternatives* 27, pp. 41-62.

Hwang, John D. (1999), “Help for Cyberterrorism: Y2K’s Silver Lining,” *IOT Profesional* 1.1, pp. 74-75.

Hynek, Nik (2018), “Theorizing International Security Regimes: A Power-Analytical Approach,” *International Politics* 55, pp, 352-365.

Iasiello, Emilio (2020), “*Is a US-Russia Cyber Security Group Silly?*, *Technative*,

International Telecommunication Union (2008), “ITU Regional Cybersecurity Forum 2008, Doha, Qatar, English Draft Meeting Report: ITU Regional Workshop on Framework for Cybersecurity and Critical Infrastructure Protection (CIIP) and Cybersecurity Forensics Workshop,” https://www.itu.int/ITU-D/cyb/events/2008/doha/docs/doha-cybersecurity-forum-report-feb-08.pdf (Accessed 21 September, 2020).

Johnston, Alastair Iain (1995a), "Thinking about Strategic Culture," *International Security* 19.1: 32-64.

Johnston, Alastair Iain, (1995b), *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History*, Princeton: Princeton University Press.

Jones, Anita K. (2006), "Cybersecurity and Urban Terrorism—Vulnerability of the Emergency Responders," in Schweitzer, Glenn E. and Chelsea Sharbe, eds., *Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop* (pp. 14-24), file:///C:/Users/willi/Downloads/11698%20(1).pdf, (Accessed 4 April, 2021).

Jones, Anita K. Jones, Anita K., Igor Fedorov, Lewis M. Branscomb, Nikolay V. Medvedev, Yury K. Shiyan, Linton Wells III, Michael Wolin, and A. Chelsea Sharbe (2006), "Report of U.S.-Russian Working Group on Cyberterrorism Issues, in Schweitzer, Glenn E, and A, Chelsea Sharber, eds., *Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop* (pp. 9-13.), file:///C:/Users/willi/Downloads/11698%20(1).pdf, (Accessed 4 April, 2021).

Jones, Frank L., Jr. (2012), "Strategic Thinking and Culture: A Framework for Analysis," in Bartholomees, J. Boone, Jr., ed., *U.S. Army War College Guide to National Security Issues*, Carlisle, PA: Strategic Studies Institute, U.S, Army War College, pp. 287-304.

Jung, Hoyoon (2019), "The Evolution of Social Constructivism in Political Science: Past to Present," *SAGE Open*, https://journals.sagepub.com/doi/pdf/10.1177/2158244019832703, (Accessed 22 April, 2021).

Karimov, Elgün (2009), “Jockeying for Power in the South Caucasus: The Interests of Russia and the United States in the Conflict in Nagorno-Garabakh,” Master’s Thesis, William Paterson University.

Katzenstein, Peter J. (), “Introduction” in Katzenstein, Peter J., ed., *The Culture of National Security: Norms and Identity in World Politics*, New York: Columbia University Press, pp, 1 - 32.

Keohane, Robert (1988). “International institutions: Two approaches,” *International Studies Quarterly* 32, pp. 379-396.

Keys, Donald (1982), *Earth at Omega: Passage to Planetization*, Boston: MA: Branden.

Kim, Young Mie (2020), *New Evidence Shows How Russia's Election Interference Has Gotten More Brazen*, Brennan Center for Justice, https://www.brennancenter.org/our-work/analysis-opinion/new-evidence-shows-how-russias-election-interference-has-gotten-more, (Accessed 24 April, 2021).

Klein, Bradley S, (1988), “Hegemony and Strategic Culture: American Power Projection and Alliance Defense Politics,” *Review of International Studies* 14.2, pp. 133-148

Kolodny, Annette (1984), Metaphor As Experience and History in American Life and Letters, Raleigh-Durham, NC: University of North Carolina Press.

Korobkov, Andrei V, and Zhanna A. Zaionchkovskaya (2012), "Russian Brain Drain: Myth vs, Reality," *Communist and Post-Communist Studies* 45.3/4, *Special Issue: Disintegration of the Soviet Union Twenty Years Later. Assessment, Quo Vadis?* (September. December), pp. 327 -341.

Korunov, Andrey and Olga Oliker, eds. (2017), *A Roadmap for U.S.-Russian Relations*, New York: Rowman and Littlefield.

Kshetri, Nir (2015), "Cybercrime and Cybersecurity in the BRICS," *Journal of Global Information Management* 18.4, pp. 245-249.

Kydd, Andrew (2006), "When Can Mediators Build Trust?" *American Political Science Review* 100.3,pp. 449-462.

Kydd, Andrew and Duncan Snidal (1997), "Progress in Game-Theoretical Analysis of International Regimes," in Hasenclever, Andreas Peter Mayer and Volker Rittberger, ed.s , *Theories of International Relations*, Cambridge: Cambridge University Press, pp. 1112-135.

Lee. Matthew (2020), "US Sanctions Turkey over Purchase of Russian Missile Defense System," *Associated Press*, 14 December, https://www.defensenews.com/pentagon/2020/12/14/us-sanctions-nato-ally-turkey-over-purchase-of-russian-missile-defense-system/, (Accessed 1 April, 2021).

Lee, Stephanie and Alexandra Silver (2014*), The Group of Eight (G8) Industrialized Nations*, *Council on Foreign Relations*, www.cfr.org/backgrounder/group-eight-g8-industrialized-nations (Accessed 12 March, 2021).

Leites, Nathan C, *The Operational Code of the Politburo*, New York: McGraw Hill, 1951.

Leonisio, Rafael, Fernando Molina, and Diego Muro (eds.) (2016), ETA's *Terrorist Campaign: From Violence to Politics, 1968-2015 (Extremism and Democracy)*, New York: Routledge.

Lewis, James A. (2017), "Cybersecurity: A U.S. Perspective," in *A Roadmap for U.S.-Russian Relations*, edited by Andrey Korunov and Olga Oliker, Washington, D.C.: Center for Strategic International Studies, pp. 62-68.

Libel, Tamir (2016), "Explaining the Security Paradigm Shift: Strategic Culture, Epistemic Communities, and Israel's Changing National Security Policy," *Defense Studies* 16.2, pp. 137-156.

Lkhagvasuren, Galbaatar (2017), *Impact of Draft International Code of Conduct for Information Security*, https://medium.com/@galbaatar_l/impact-of-draft-international-code-of-conduct-for-information-security-8cfe3742cc5b, (Accessed 1 April 2021).

Lotrionte, Catherine and Tim Maurer (2012), "Introduction: Building Trust in Cyberspace," *Gerogetown Journal of International Affairs, Special Issue--International Engagement on Cyber 2012: Establishing Norms and Improving Security*, pp. 1-4.

Mahmadi, Aamer, Mathew Lee. And Zeynep Bilginsoy (2021), *Biden Recognizes Atrocities against Armenians As Genocide*, Associated Press (24 April), https://apnews.com/article/joe-biden-turkey-government-and-politics-middle-east-europe-dbe6bc9ddac90c1393e6c33ff2220781, (Accessed 25 April, 2021).

McConnell, Bruce W., Pavel Sharikov, and Maria Smekalova (2017), *Suggestions on Russia-U.S. Cooperation in Cybersecurity*, Russian International Affairs Council/EastWest Institute, https://www.eastwest.ngo/sites/default/files/RIAC-EWI-Russia-US-Cybersecurity-Policybrief11-en.pdf, (Accessed 4 March, 2021.

McKune, Susan, (2015), *An Analysis of the International Code of Conduct for Information Security*, Toronto: Munk School, University of Toronto, https://openeffect.ca/code-conduct/, (Accessed 4 April 2021).

"Merkel Calls Obama about US 'Spying on Her Phone'" (2013), *BBC News*, https://www.bbc.com/news/world-us-canada-24647268, (Accessed 22 March, 2021). (Accessed March, 2020).

Miller, Robert (2006), *Native America, Discovered and Conquered: Thomas Jefferson, Lewis and Clark, and Manifest Destiny,* Westport: CT: Praeger, 2006.

Ministry of Foreign Affairs of the Russian Federation (2016), *Doctrine of Information Security of the Russian Federation*, 5 December, https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163n (Accessed 22, September 2020.

Moens, Alexander, Seychelle Cushing, and Alan W. Dowd (2015), *Cybersecurity Challenges for Canada and the United States*, Vancouver, Fraser Institute, https://www.fraserinstitute.org/sites/default/files/cybersecurity-challenges-for-canada-and-the-united-states.pdf, (Accessed 4 September, 2020).

Montville, Joseph V. (2992), “Track Two Diplomacy: The Arrow and the Olive Branch: A Case for Track Two Diplomacy,” in Volkan, Vamik D. Voltam, and Demetrios A. Julius, eds., *The Psychodynamics of International Relations*, Vol. 2, Unofficial Diplomacy, Lanham: MD: Lexington, pp. 161-175.

Moore, Joe Wesley (2002), “Information Warfare: Cyberterrorism and Community Values,” LLM thesis, Faculty of Law, Institute of Air and Space Law, McGill University, file:///C:/Users/willi/Downloads/458383.pdf (Accessed 4 September, 2020).

Moscow in Talks with US to Create Cybersecurity Working Group: RIA Report, (2017). Reuters 20 July, https://www.reuters.com/article/us-russia-us-cyber-envoy/moscow-in-talks-with-u-s-to-create-cyber-working-group-ria-report-idUSKBN1A51MM, (Accessed 24 April, 2021).

Munir, Zeesham and Raju Keshari (2018), “Russia as a Factor in India-China Relations,” *World Affairs: The Journal of International Issues*, 22.2: pp. 94-105.

Natho, Kadir I, *Circassian History*, Bloomington, IN: Xlibris.

National Research Council (1991), *Computers at Risk: Safe Computing in the Information Age*. Washington, D.C.: The National Academies Press.

NATO (2016a) *Cyber Defense Pledge* (8 July), https://www.nato.int/cps/en/natohq/official_texts_133177.htm, (Accessed 13 March, 2021).

NATO (2016b), *Warsaw* Summit Comminiqué, https://www.nato.int/cps/en/natohq/official_texts_133169.htm, (Accessed 4 March, 2021).,

NATO (2018), *Brussels Summit Declaration*, https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/Multilateral/NATO+Brussels+Summit+Declaration.pdf, (Accessed 31 March 2021).

New York Times Editorial Board (2014), "Edward Snowden, Whistle Blower, *New York Times* 1 January, https://www.nytimes.com/2014/01/02/opinion/edward-snowden-whistle-blower.html, (Accessed 22 March, 2021).

Nocetti, Julein (2015), "Contest and Conquest: Russia and Global Internet Governance," *International* Affairs 91.1, pp. 111-138.

"NSA Monitored Calls of 35 World Leaders," *The Irish Times* 25 October, , https://www.irishtimes.com/news/world/europe/nsa-monitored-calls-of-35-world-leaders-1.1572561, (Accessed 12 March, 202).

Nye, Joseph S., Jr. (1987), "Nuclear Learning and U.S.-Soviet Regimes," *International Organization* 41.3, pp. 371-402.

“Obama Calls Hollande to Promise U.S Is No Longer Spying on French President,” *The Guardian* (24 June 2015), https://www.theguardian.com/world/2015/jun/24/obama-calls-hollande-nsa-no-longer-spying-french-president, (Accessed 22 March, 2021).

Pasley, James F, (2003), “United States Homeland Security in the Information Age: Dealing with the Threat of Cyberterrorism,” *White House Studies* 3.4, pp. 403-410.

Pavlov, Alexander and Vladimir Rybachenkov (2013). “Looking Back: The U.S.-Russian Uranium Dean—Results and Lessons,” *Arms Control Association*, https://www.armscontrol.org/act/2013-12/looking-back-us-russian-uranium-deal-results-lessons#:~:text=In%20February%201993%2C%20Russia%20and,over%20a%2020%2Dyear%20period, (Accessed 4 April, 2021).

Prashad, Krishna (2012), “Cyberterrorism: Addressing the Challenges for Establishing an International Legal Framework.” Paper presented at the Australian Counterterrorism Conference, 12 March, 2012. https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1016&context=act, (Accessed 12 September, 2020).

Price, Richard and Christian Reus-Smit, (1998), “Dangerous liaisons? Constructivism and Critical International Theory.” *European Journal of International Relations* 4, 259-294.

Prokopeva, Viktoria Andreyevna (2017), “Politika protivodyeistviya kiberterrorizmu v sovremyenonnoi Rossii’ (Countering Cyberterrorism in Contemporary Russia), qualifying dissertation, Ural State Pedagogical University, Faculty of International Relations and Social and Humanitarian Communications,Yekaterinburg: Russia.

Propp, Kenneth (2019), "US Surveillance on Trial in Europe: Will Transatlantic Digital Commerce Be Collateral Damage?" *Atlantic Council* (September), https://www.jstor.org/stable/resrep26699, (Accessed 24 March, 2021).

Putin Says Snowden Was Wrong to Leak Secrets. But Is No Traitor (2017), https://www.reuters.com/article/us-russia-putin-snowden/putin-says-snowden-was-wrong-to-leak-secrets-but-is-no-traitor-idUSKBN18T1T4, (Accessed 22 March, 2021).

Radikow, Ivan V. (2019), "Trust in the Cooperation between the Citizens and the State in Contemporary Russia," *Politcja* 62: pp. 33-50.

Rand, Ayn (1964), *The Virtue of Selfishness*, New York: Signet.

"Regulation (EU) 2016/679 of othe European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)." *Office Journal of the European Union,* 27 April, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679, (Accessed 26 March, 2021).

République de la France, Ministére de l'Europe et des Affaires Étrangères (2021), *Statement of G7 Leaders on Ukraine*, https://www.diplomatie.gouv.fr/en/country-files/ukraine/news/article/g7-foreign-ministers-statement-18-03-21, (Accessed 31 March, 2021).

Rid, Thomas (2011), *Cyber War Will Not Take Place*, Oxford, Oxford UP.

Roche, Edward M. and Michael J. Blaine (2014), "International Convention for the Peaceful Use of Cyberspace," *Orbis* 2, pp. 282-296.

Rubin, Josh (2019), "NATO Fears That This Town Will Be the Epicenter of Conflict with Russia," *The Atlantic* 4 January, https://www.theatlantic.com/international/archive/2019/01/narva-scenario-nato-conflict-russia-estonia/581089/, (Accessed 22 March 2021.

Ryan, Lucas (2021), *FBI Defends Agency in Testimony, Calls Jan. 6 Attacks "Domestic Terrorism*," National Public Radio WNYC (2 March), https://www.npr.org/2021/03/02/972970812/fbi-director-defends-agency-in-testimony-calls-jan-6-attack-domestic-terrorism (Accessed 23 March 2021).

Saad, Lydia (2019), *Majority of Americans Now Consider Russia a Critical Threat*, Gallup (27 February), https://news.gallup.com/poll/247100/majority-americans-consider-russia-critical-threat.aspx, (Accessed 31 March, 2021).

Schmitt, Michael N., ed. (2013), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf, Accessed 13 November 2021.

Schweitzer, Glenn E. and Sharber, A. Chelsea, eds. (2006) *Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop*, Washington, D.C., The National Academies Press.

Shad, Mohammed Riaz (2018), "Cyber Threat in Interstate Relations: Case of US-Russia Cyber Tensions." *Policy Perspectives* 15.2, 41-55.

Shaffer, Helen B. (2021), "Cultural Exchanges with Soviet Russia," *CQ Researcher*, https://library.cqpress.com/cqresearcher/document.php?id=cqresrre1959070300, (Accessed 22 February 2021.

Shanghai Cooperation Organization (2009), *Agreement between the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of Information Security*, https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Multilateral/Shanghai+Cooperation+Organization+Agreement+on+Cooperation+in+the+Field+of+International+Information+Security+6-16-2009.pdf, (Accessed 26 March, 2021).

"Shanghai Five Nations Sign Joint Statement" (2000), *People's Daily* 06 July, http://en.people.cn/200007/06/eng20000706_44803.html, Accessed 7 March, 2021.

Sharikov, Pavel (2017), "Cybersecurity: A Russian Perspective," in *A Roadmap for U.S.-Russian Relations*, edited by Andrey Korunov and Olga Oliker, Washington, D.C: Center for Strategic International Studies, pp. 69-72.

Smale, Allison and Michael D, Shear (2014), “Russia is Ousted from Group of 8 by U.S. and Allies,” *New York Times* 24 March, https://www.nytimes.com/2014/03/25/world/europe/obama-russia-crimea.html, (Accessed 26 March 2021).

Snyder, Jack L. (1977)*, The Soviet Strategic Culture: Implications for Limited Nuclear* Operations-- R-2154-AF, Santa Monica, CA: RAND Corporation, September.

“Soviet Cult Film *Moscow Does Not Believe in Tears”* (nd), *Soviet Art/USSR Culture*, https://soviet-art.ru/soviet-cult-film-moscow-does-not-believe-in-tears/, (Accessed 13 March, 2021).

Stent, Angela (2018), “The Sino-Russian Partnership and Its Impact on U.S. Policy toward Russia,” *Asia Policy* 13.1, 5-11.

Stevens, Tim (2017), “Cyberweapons: An Emerging Global Governance Architecture,” Palgrave Communications document, DOI: 10.1057/palcomms.2017.4, https://www.nature.com/articles/palcomms2016102,(Accessed 4 March, 2021).

Stevens, Tim (2018). “Cyberweapons: Power and the Governance of the Invisible,” *International Politics* 55, pp. 482-502.

Streltsov, Anatoly (2012), “Confidence-Building Measures: The Future of the Global Information Infrastructure,” *Georgetown Journal o fInternational Affairs: --Special Edition-- International Engagement on Cyber*: *Establishing Norms and Improving Security,* pp.25-33.

Střítecky, Vitek and Nik Hynek (2018), "Comparing Global Security Regimes: A Power-Analytical Synthesis, *International Politics* 55, pp. 503-517.

Tabaksky, Lior (2013), "Does Cyberspace Promote Human Rights and Democracy? Applying Karl Popper's Scientific Method," *The International Journal of Science in Society* 4, pp. 13-23.

Troianovsky, Anton (2021), "Moscow Erupts in Fury over Biden Calling Putin a Murderer, *The New York Times* 18 March, https://www.nytimes.com/2021/03/18/world/europe/russia-biden-putin-killer.html, (Accessed 4 April 2021).

Tsai, Yu-tai (2009), "The Emergence of Human Security: A Constructivist View," *International Journal of Peace Studies*, 14.2, pp. 19-33.

United Nations (1966), *International Covenant on Civil and Political Rights*, https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf, (Accessed 4 March 2021).

United Nations General Assembly (2010), *Resolution Adopted by the General Assembly on 8 December 2010 [on the report of the First Committee (A/65/405)] 65/41. Developments in the Field of Information and Telecommunications in the Context of International Security*, https://undocs.org/en/A/RES/65/41, (Accessed 17 March, 2021).

United Nations, General Assembly (2011*), Code of Conduct for International Security--Annex to the letter dated 12 September 2011 from the Permanent Representatives of China, the*

Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, file:///C:/Users/willi/Downloads/A_66_359-EN%20(1).pdf, , (Accesssed 5 March, 2021).

United Nations General Assembly (2015a), *Code of Conduct for International Security --Annex to the letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, file:///C:/Users/willi/Downloads/A_69_723-EN%20(1).pdf, (Accessed 1 April 2021).

United Nations General Assembly 2015b, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (2015b), file:///C:/Users/willi/Downloads/A_70_174-EN%20(2).pdf, (Accessed 4 March 2021).

United Nations, Department of Economic and Social Affairs (2021), *World Summit on the International Society (WSIS): WSIS Action Lines Supporting the Implementation of SDGS—Outcomes*, https://sustainabledevelopment.un.org/index.php?page=view&type=30022&nr=102&menu=3170, (Accessed 24 April, 2021).

Urbina, Ian (2009), "Thousands Hold Peacebul March at G-20 Summit," *New York Times* 25 September, https://www.nytimes.com/2009/09/26/world/26pittsburgh.html, (Accessed 26 March, 2021).

US Department of State (2020), *Fact Sheet: U.S, Support for Digital Transformation in Latin America and the Caribbean*, 10 November, https://do.usembassy.gov/fact-sheet-u-s-support-for-digital-transformation-in-latin-america-and-the-caribbean/, (Accessed 22 February 2021).

US Department of State (2021), *New START Treaty*, https://www.state.gov/new-start/, (Accessed 4 February 2021).

US Embassy in Georgia (2020), "US Helps Allies Fight Cyberattacks," 26 August, https://ge.usembassy.gov/u-s-helps-allies-fight-cyberattacks/, (Accessed 11 September 2020).

US Federal Trade Commission (2015), "Update on the Safe Harbor Framework" 25 July, https://www.ftc.gov/tips-advice/business-center/guidance/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor, (Accessed24 March, 2021.

US National Intelligence Council (2021), "Foreign Threats to the 2020 US Elections" (15 March), https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf, (Accessed 4 April 2021).

US Senate Intelligence Committee (2018), "New Reports Shed Light on Internet Research Agency's Social Media Tactics," 17 December, https://www.intelligence.senate.gov/press/new-reports-shed-light-internet-research-agency%E2%80%99s-social-media-tactics, (Accessed 1 April, 2021).

Uz-Zaman, Rashed (2009), "Strategic Culture: A 'Cultural' Understanding of War," *Comparative Strategy* 28.1, pp. 68-88.

Vygotsky, Lev (1976), *Mind in Society*. Cambridge, MA: Harvard University Press.

Weaver, Ole, Barry Buzan, Morten Kelstrup, and Pierre Lemaitre (1993). *Identity. Migration, and the New Security Agenda in Europe*. London: Pinter.

White House, Office of the Press Secretary (2014), *Statement of G7 Leaders on Ukraine*, https://obamawhitehouse.archives.gov/the-press-office/2014/03/12/statement-g-7-leaders-ukraine, (Accessed 26 March 2021).

Williams, Raymond (2018, "The Analysis of Culture," In Storey, John, ed. *Cultural Theory and Popular Culture: A Reader*, New York: Routledge, pp. 45-49.

Wiltenburg, Ivor (2020), "The Importance of Understanding Russian Strategic Culture," *Atlantisch Perspektief* 44.1, pp. 7-12.

Wortman, Richard (1987), *The Making of Three Russian Revolutionaries: Voices from the Menshevik Past*, Cambridge: Cambridge University Press.

Yamin, Tughral (2015), "Combating Cyber Terrorism through an Effect System of Cyber Security Cooperation" (unpublished), paper presented at the Terrorism Experts Conference, Ankara, November 2015), https://www.researchgate.net/publication/303255678_Combating_Cyber_Terrorism_through_an_Effective_System_of_Cyber_Security_Cooperation, (Accessed 4 November 2020).