Countering & Preventing Russian Cyberattacks

Katharine E. Hastings
Frank Batten School of Leadership & Public Policy

Applied Policy Project, April 2022

Written for the Foundation for Defense of Democracies

ACKNOWLEDGEMENTS

I would like to express my sincerest thanks to Annie Fixler, Deputy Director, Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies. While I had a strong interest in the cyber security and the emerging threats posed by ransomware, I did not possess the knowledge of cyber diplomacy. I consulted dozens of research publications, reports, and think pieces to provide me with a base of knowledge on the evolving threat posed by cyberattacks. My original thesis had focused on the global cyber threat posed by nation-states in general and Ms. Fixler was instrumental in framing and focusing my research. She provided me insights and guidance to specifically target Russia and its efforts to undermine U.S. national security and infrastructure. She also shared important research that helped me develop and define my policy options. I owe her a great debt of gratitude for completing this project.

I also want to thank Robert Popovich for being a great mentor to me. His foreign policy experience and expertise interacting with military and intelligence officials in the Soviet Union coupled with the voluminous resources he shared were invaluable in my understanding of the issues involved. He provided unique insights into the dynamics of the U.S.-Russian relationship that proved critical in my analysis.

I would like to extend a special thanks to the Batten School of Leadership and Public Policy and its faculty. This Applied Policy Project is the culmination of my graduate studies. I have incorporated what I have learned from nearly every course. In particular, I want to thank Professor Gerald F. Warburg who helped me hone my policy briefing skills, and for my APP academic advisor, Professor Allan Stam, for his assistance in helping me navigate this complex subject. Also, my fellow students provided me with critical feedback that helped improve the quality of my work.

Finally, I want thank my mother and father who have always been my strongest supporters and inspired me to pursue my MPP. They have not only cheered me on but they have instilled in me the characteristics of hard work, determination, and integrity. Completing this project has been an experience I will never forget, and their love, advice and understanding has been priceless.

Katharine Hastings

DISCLAIMER

The author conducted this study as part of the program of professional education at the Frank Batten School of Leadership and Public Policy, University of Virginia. This paper is submitted in partial fulfillment of the course requirements for the Master of Public Policy degree. The judgments and conclusions are solely those of the author, and are not necessarily endorsed by the Batten School, by the University of Virginia, or by any other agency.

HONOR PLEDGE

On my honor as a student at the University of Virginia, I have neither given nor received aid on this assignment.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Russian cyberattacks continue to increase, have become more sophisticated, and threaten our national security and infrastructure. From ransomware attacks, election interference, corporate espionage, and threats to the electric grid, these acts pose grim implications not just for cyberspace but also for economies, geopolitics, and fundamental questions of war and peace. Russia and its proxies are well funded and often engage in sophisticated, targeted attacks. They are primarily motivated by political, economic, technical, or military agendas, with a range of goals that vary at different times. For example, Russia frequently engages in industrial espionage, and they have conducted ransom attacks and electronic thefts of funds. Furthermore, Moscow may employ hackers to attack U.S. and European networks in retaliation against sanctions in response to their invasion of Ukraine (Robertson, 2022).

How does the U.S. address this threat which is unconfined by geography, can be initiated at the flip of a switch, and is difficult to attribute and prosecute the source of the attack? What policy options can stem the tide, if not reduce, the frequency and impact of cyberattacks?

In addressing these issues, this analysis draws on current diplomatic efforts in the cyber arena with a specific focus on U.S. and Russian cyber policies. My research evaluated three policy alternatives to address this threat: (1) developing and defining cyber norms, (2) banning cyberattacks on critical infrastructure, and (3) cooperation against cybercrime. The level of collaboration and mutual interest varies, and the following criteria were used to evaluate the different policy options:

- **Transparency:** Assess the coordination between Russia and the U.S. in identifying sources of cyberattacks.
- **Security:** Assess the reduction in the number of successful attacks on critical infrastructure targets.
- **Accountability:** Assess the number of hackers identified, financial losses reduced, cases prosecuted, and criminals extradited to the U.S. or sent to prison.
- **Cost:** Assess the financial costs for the U.S. to implement each option.
- **Political Viability:** Assess the likelihood that the U.S. and Russia will reach a bilateral agreement on the policy

RUSSIAN INVASION OF UKRAINE

The recommendations in this report are severely constrained due to Russia's invasion of Ukraine. The U.S., along with its European allies and dozens of other nations, have suspended diplomatic relations and imposed the most extensive and punitive economic sanctions on Russia and its elites. The U.S. and its allies have also extended billions in military and humanitarian aid to Ukraine. Any discussions or diplomatic outreach of the proposed policy options are on hold until this crisis is resolved.

I recommend that the U.S. pursue the second policy alternative -- ban cyberattacks on critical infrastructure in peacetime. Coupled with strong deterrent threats and the federal government allocating financial and technical resources to harden our infrastructure, this policy will reduce the frequency and intensity of attacks by Russia and its proxies. Both Russia and the U.S. have a mutual self-interest in this domain. Although it is costly to implement, the potential damage resulting from an attack and lives at risk is incalculable.

Reaching an agreement between the U.S. and Russia requires bringing leaders from the entire foreign policy, defense, and intelligence communities to the table. The negotiation terms and objectives must be clear and realistic. The U.S. should also pursue a parallel track with its European and NATO allies by keeping them informed and engaged to maximize diplomatic pressure.

(Word Count: 9,693)

PROBLEM STATEMENT

Russia has emerged as the United States' most malicious and persistent cyber threat. According to the U.S. Office of the Director of National Intelligence 2021 Annual Threat Assessment, "Russia almost certainly considers cyberattacks an acceptable option to deter adversaries, control escalation, and prosecute conflicts" (ATA, 2021). Despite U.S. efforts to strengthen our capability, readiness, and resilience in cyberspace, *Russian cyberattacks continue to increase, become more sophisticated, and threaten our national security and critical infrastructure.*

INTRODUCTION

Cyber's Unique Challenges

The cyber threat poses unique challenges. Among the special characteristics of the cyber-domain are the erosion of distance, the speed of engagement, the low cost of cyberweapons, and the difficulty of attribution. Cyberspace is a unique phenomenon where domestic and international issues are so closely intertwined that it is almost impossible to explore one without the other. Cybersecurity blurs the lines of public and private vulnerabilities. Unlike conventional or nuclear weapons, the government does not control them, and unlike military security, the Pentagon plays only a partial role. For example, cybercriminals may pose as serious a threat to national security as any military source. The new system of international relations features new categories of actors and new forms of interaction within the borderless cyber domain, thus challenging the very idea of sovereignty.

A primary problem in finding diplomatic solutions involves the attribution of cyberattacks. There is no international mechanism of attribution that would provide the possibility to investigate, prosecute, prevent, or punish states, entities, or criminals who commit a cyberattack (McConnell et al., 2017). This allows deniability and slows retaliatory responses. Further complicating matters is whether the proper retaliation, be it proportional or asymmetrical, is confined to the cyber realm or if a kinetic, economic, or political response is warranted. A retaliatory strike may result in an escalatory response, potentially harmful, and cause inadvertent damage to outside parties.

Differing U.S.-Russian Worldviews

Another challenge are the differing U.S. and Russian views of the Internet, information exchange and cybersecurity. Russia focuses its national information security efforts on protecting society from "harmful" information (Van Epps, 2013). The U.S. views information as a public good, which should be subject to minimal controls and allowed to flow as freely as possible. In contrast, Moscow worries about the unrestricted exchange of information having a destabilizing effect on its society and undermining the rule of the current leadership. The ability of the government to monitor and control the information domain is an essential component of the Russian position on cybersecurity and its international efforts on cyber issues.

Given this distressing reality, any suggestions to identify and agree upon rules of the road in cyberspace are met with skepticism. Conventional wisdom states that the core attributes of cyberspace make it all but impossible to enforce any norms or even to know if they are being violated in the first place. While Russia and the U.S. may view cybersecurity differently, taking advantage of the commonalities that do exist is necessary to forge a broader agenda on cybersecurity. Several points of agreement provide a starting point for cooperation, including protecting critical infrastructure, sharing information on threats, and combating ransomware and other criminal activity.

CLIENT OVERVIEW

The Foundation for Defense of Democracies (FDD) is a nonpartisan research institute focusing on national security and foreign policy. FDD's Center on Cyber and Technology Innovation (CCTI) has a particular interest in countering cyber threats. The cyber domain provides new avenues for state and non-state actors to undermine U.S. national security and democracy. The U.S. and its adversaries are shaping the battlefield of cyberspace and international norms through their actions. CCTI has been at the forefront in identifying how America's authoritarian, undemocratic adversaries are using cyber tactics to undermine the foundation of our nation's institutions and infrastructure as a means to weaken us politically and militarily. FDD believes American engagement and active cooperation with our allies are essential to defend U.S. national interests in cyberspace, reducing or eliminating threats posed by adversaries and capitalizing on the opportunities provided by emerging technology.

FDD seeks interdisciplinary research to identify technological, governance, and policy solutions in reducing or eliminating threats posed by adversaries and enemies of the U.S. and other free nations. Through the production of actionable research, prepared by experts and scholars from various backgrounds - including government, intelligence, military, private sector, and academia - FDD provides policy options and analysis to policymakers to advance U.S. national security interests.

There is a solid foundation of international law and theory to explore. FDD has encouraged me to focus on what is possible and practical in the near term. There are interrelated points of common interest and norms of behavior between the U.S. and Russia that can lead to tangible diplomatic initiatives that can be adopted.

BACKGROUND ON THE PROBLEM

Cyberspace went global in 1990 when Tim Berners-Lee invented the World Wide Web. In its formative years, the web's open access to information, social interaction, and commerce aligned with Western values.

These values, however, also proved a threat to authoritarian regimes who worried that their hold on power would be undercut by digital-age capabilities empowering civil society. The Arab Spring that swept through North Africa and the Middle East in 2011 was a watershed event. Autocratic regimes that felt threatened by social media and an open internet now had to respond. They did so clumsily at first, trying to shut down internet service providers or block social media sites. Regimes like Iran quickly realized cyber's offensive capabilities by mounting surveillance efforts against their citizens to locate their adversaries and monitor their planning (Thomson Reuters, 2010).

Cyber-enabled intellectual property theft was the most common threat for many years, but state-sponsored malicious activities evolved to impose significant costs on the public and private sectors. For example, in 2010, the Stuxnet computer worm, allegedly developed by Israel and the U.S., became the first known virus capable of crippling hardware. Originally targeted at Iran's nuclear facilities, Stuxnet and its prodigy have mutated and spread to other industrial and energy-producing facilities (Fruhlinger, 2017). These and other events showcased the inseparability of cyberspace's domestic and international aspects.

Gen. Michael Hayden, former Director of the NSA and CIA, realized the significance of this event and its effects in cyberspace. In his view, a state actor "had just used a weapon composed of ones and zeros, during a time of peace, to destroy what another nation could only describe as critical infrastructure…Someone had crossed a Rubicon…We were in a new military age" (Hayden, 2016).

Cyber: The Fifth Domain

In 2010, cyber was defined by the Department of Defense (DOD) as the "fifth domain" of warfighting (Schneider, 2020), joining land, sea, air, and space. Concurrently, the DOD created U.S. Cyber Command (USCYBERCOM) to address cyber threats to U.S. military forces and strengthen our nation's ability to withstand and respond to cyberattacks. A key component of USCYBERCOM's mission was maintaining U.S. superiority in cyberspace, offsetting our adversaries' developments, and responding to any attacks of significant consequence against our nation's critical infrastructure.

The U.S. military viewed cyberspace as a venue specifically for state-on-state conflict dominated policymaking and strategy. Secretary of Defense Leon Panetta ominously warned in 2012 of a "cyber Pearl Harbor" (Bumiller, 2012). Panetta described a major cyberattack on industrial control systems that could disable the nation's power grid, transportation system, financial industry, and government.

Panetta's fears appeared valid, and 2013 marked "a strategic inflection point" (Schneider, 2020). U.S. adversaries developed new ways to mount continuous, nonviolent operations that produced cumulative, strategic impacts. By strategically targeting private sector entities and avoiding military sites, nation-states mounting these cyber campaigns took care to operate in ways that would not trigger an armed U.S. response (Nakasone, 2019). Examples of their assaults included:

- Iranian denial-of-service attacks against the financial sector (2012–2013)
- Attack on the Sands Casino (2014)
- North Korea's attack on Sony Pictures Entertainment (2014), and
- China's disruption of GitHub (2015) and theft of security-related data from the Office of Personnel Management (2015).

The most prominent campaign involved Russia's disinformation efforts to interfere with the 2016 American presidential election. These campaigns were not isolated hacks or incidents but strategic campaigns. The objective for each attack was to erode U.S. military, economic, and political power without reaching a threshold that triggered an armed response. Russia and China began stealing unprecedented quantities of intellectual property and personal data, disrupting democratic processes, and threatening the integrity of critical infrastructure. They demonstrated that cyberspace activities over time could cumulatively erode and undermine a country's sources of national power without firing a shot.

Deterrence and Why it Failed in Cyberspace

Historically, the design and deployment of new weapons -- from aircraft to chemical and nuclear weapons -- have often posed the need to define new strategies to deter their use (Taddeo, 2017). This was also the case with the emergence of cyber weapons. Military and national security experts promoted the adoption of the Cold War's theory of deterrence to meet the threat posed by cyberattacks. The theory's success in preventing a nuclear war appeared to be ideally suited against an uncontrolled and unprovoked cyberattack and to maintain international stability. As a result, deterrence was implemented during George W. Bush's administration and re-affirmed in President Obama's 2011 International Strategy for Cyberspace and the 2015 DOD Cyber Strategy.

In practice, however, deterrence proved ineffective due to the distinct nature of cyberspace. Cyber conflicts differ radically from violent military conflicts and occur in domains that are the opposite of those for which deterrence theory was developed. A nuclear attack is a singular catastrophic event, and nuclear deterrence aims to prevent its occurrence. In contrast, cyberattacks are frequent and persistent, and deterring them is more akin to deterring ordinary crime: the goal is to keep it within limits (Nye, 2022).

As the table below illustrates, deterrence was predicated on specific conditions to be successfully implemented, each of which is absent in cyberspace (Morgan, 2003).

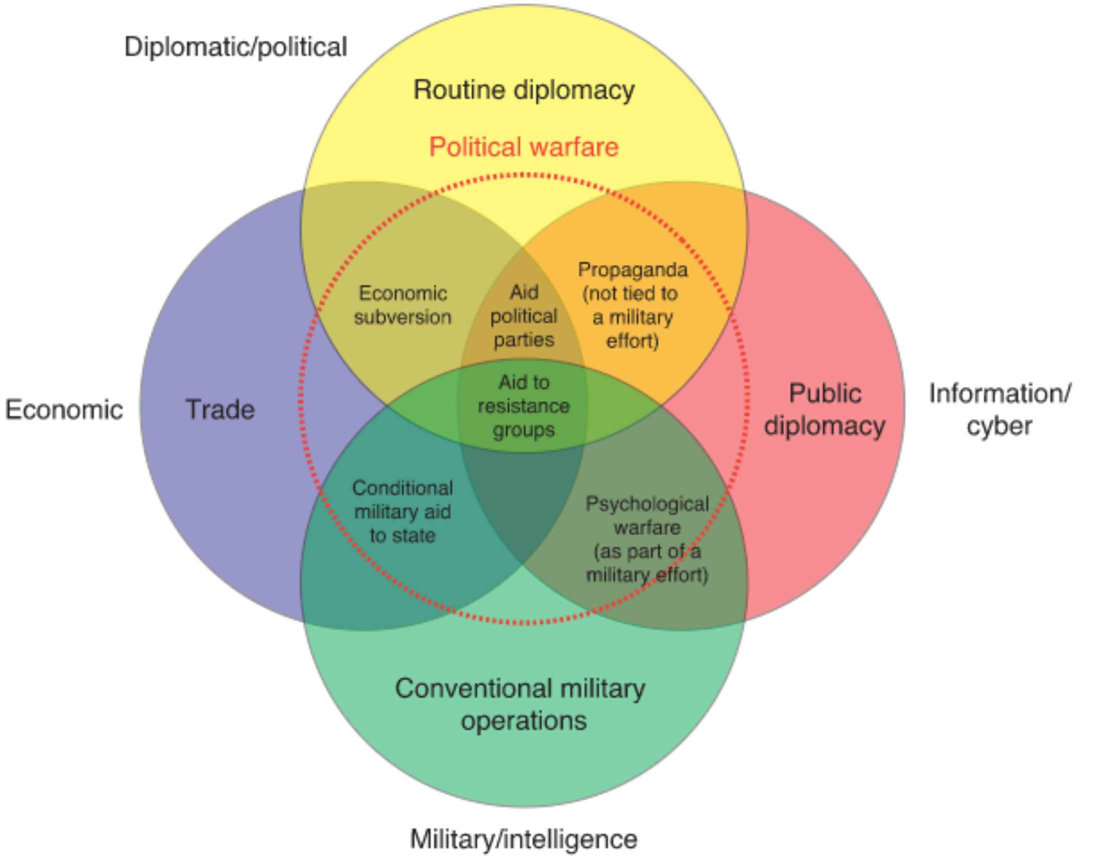
Table 1. Deterrence vs. Cyber Domain

Deterrence Domain	Cyber Domain
Prevailing kinetic military conflict typically between two nation-states.	Non-kinetic cyber operations among multiple nation-states and/or non-state actors.
Applies rational choice models to identify strategies among the adversaries.	Cost-benefit analysis varies depending on the nature of attack.
Attribution of attackers is clear.	Non-symmetrical, multi-laterals interactions, attribution often unclear or unknown.
Singular retaliation that is sufficient to inflict severe punishment on the opponent.	Ever-changing dynamics of response, persistent attacks, and counter-attacks.
Clear demonstration of the defender's capabilities.	Ambiguity, rather than certainty.
Full control over retaliation.	Limited to no control over retaliation and its effects.

Applying traditional deterrence theory to cyberspace proves to be problematic. Treating cyberspace as a geographic territory or comprised of physical assets such as computer components failed to address the pervasive nature of the threat. With nuclear weapons, deterrence helped frame the Nuclear Test Ban Treaty, the Strategic Arms Limitation Treaties, Anti-Ballistic Missile Treaty, and other non-proliferation initiatives. Hacking and encryption are based on algorithms, psychological influence, deception, and other factors. A treaty cannot ban or limit mathematics.

Cyber continues to evolve into an all-encompassing aspect of everyday life and is embedded in the framework of each military domain (Kreuzer, 2021). As highlighted in Figure 1 below from the RAND Corporation, cyber is functionally integrated within all political, economic, and military power components. Cyberspace is "a layer on top of our existing reality," permeating all equipment across all domains of warfare (Morgan, 2014). As a result, deterrence is mismatched against the unique capabilities of cyberspace, which generates continuous tactical, operational, and strategic attacks.

Figure 1. Where Cyber Warfare Fits Within the Implements of Power



Source: Robinson, L., Migacheva, K., Magnuson, M., Radin, A., Nader, A., Cohen, R. S., & Helmus, T. C. (2019). *The Growing Need to Focus on Modern Political Warfare* (p. 2, Issue brief). Santa Monica, CA: RAND Corporation. doi:https://doi.org/10.7249/RB10071

With evidence mounting after 2013 that deterrence strategies were ineffective against most cyber aggression, U.S.CYBERCOM grew frustrated with the theory and sought alternatives. As cyber security defense expert Richard Harknett observed, “We have become very comfortable with this [deterrence] framework because it worked in the nuclear environment and still does. But this was a specific strategic response to a specific strategic environment, and it does not hold that it will be universally effective across all weapon types (Williams, 2017).

What further distinguishes the current challenge from the Cold War is that U.S. adversaries actively seek to contest American advantages and interests below the level of war. In particular, there are three unique threats to the U.S. posed by great-power competition in cyberspace:

- cyber-enabled influence campaigns that undermine public trust in and legitimacy of U.S. institutions
- the erosion of the U.S. innovation base, particularly national security technologies and theft of intellectual property
- disruptive or destructive campaigns targeting critical infrastructure and key resources.

The relatively low entry cost and the high chances of success make cyber weapons an attractive option for state and non-state actors to assert their power and authority. Cyberattacks often cause significant disruption to their adversaries without an armed response. Cyberattacks pose serious risks of escalation and invite frictions and tensions that may lead to the sparking of new cyber conflicts, which could intensify and jeopardize international stability (Taddeo, 2017).

A "Cyber Pearl Harbor" - Rhetoric vs. Reality

The worst-case scenario projected by policymakers is that an unwanted conventional or nuclear war could happen without proper rules of engagement[1] in the cyber theater (Lancelot, 2020). But are the doomsayers correct? Evidence suggests that the escalatory risks of cyberwarfare are exaggerated (Heritage Foundation, 2019). The Cato Institute analyzed 272 documented cyber exchanges between rival states between 2000 and 2016. In categorizing those exchanges, the vast majority were termed as either disruptions (33%) or espionage (54%), with only 13% considered degradation meant to disable or fundamentally damage their targets (Valeriano and Jensen, 2019).[2]

Most importantly, the researchers concluded that over two-thirds of attacks did not result in a retaliatory response. Even in those cases of retaliation, the responses tend to be proportional in matching the severity of the initial attack.   For example, Cato found that cyber operations have not been escalatory or effective in achieving a dramatic or decisive outcome (Valeriano et al., 2019). Instead, the evidence suggested "a restrained domain with few aggressive attacks that seek a dramatic impact" (Valeriano et al., 2019).

Cyberattacks are predominantly efforts to conduct surveillance, espionage, and disruption versus degrading or disabling systems or physical harm. Rarely does a response generate an increase in severity. Instead, the evidence indicates that counter-responses are of a similar or lower level

[1] "Rules of engagement" are defined as the orders issued by a competent and legitimate military authority that delineate when, where, how, and against whom military force may be used, and they have implications for what actions soldiers may take on their own authority and what directives may be issued by a commanding officer. An example includes the U.S. Marine Corps' Law of War/Introduction to Rules of Engagement (U.S.MC B130936) and The Geneva Conventions and their Additional Protocols (ICRC, 2014).

[2] To date, no cyberattack has caused mass casualties of military personnel or civilians which would typically necessitate a military response. The harm caused by espionage and disruption impacts private sector entities and individuals. It is measured in financial loss (often remediated via insurance or other means) or data loss (often recovered or restored).

than the original intrusion (Valeriano et al., 2019), or nation-states impose penalties targeting the specific individuals involved through sanctions or legal indictments.

Skeptics argue that since no one had died because of a cyberattack, it remains less important than the traditional domains of warfare. However, that position is becoming increasingly difficult to support. Cyber threats cannot be strictly viewed in a militarized sense. Cyberattacks have moved beyond the battlefield targeting these softer targets, undermining public confidence in government to deliver essential services, and threatening the lives and welfare of ordinary Americans. In 2017, the WannaCry ransomware attack damaged the British National Health Service, left computers encrypted and unusable, and forced thousands of patients' appointments and surgeries to be canceled (Nye, 2022). Hospitals and vaccine producers have also been directly targeted by ransomware attacks and hackers during the COVID-19 pandemic.

In our increasingly digital world, cloud computing is embedded within our nation's critical infrastructures. These include our electrical grid, water treatment plants, and nuclear facilities, and if attacked or compromised, could threaten the general public's health and safety. If this cyber arms race continues to expand unchecked, it would counteract the economic and social gains in this new digital world and threaten the global economy and integrity of our socio-political system.

A lack of understanding and strategy by political and military leaders regarding the nature of cyberspace could lead to a sustained escalation of cyberattacks between nation-states. On the kinetic battlefield, military weaponry is finite, and personnel must disengage and rotate. In the cybersphere, algorithms are unlimited, their deployment is automated, and they pursue their target without pause. There is a growing recognition among Washington's foreign policy community that the distribution of power in the international system has shifted in a way that disadvantages the United States. The U.S. must position itself to secure a favorable international environment that reflects its interests and values. Thus, new strategic paradigms have been proposed to more effectively protect U.S. security in the cyber landscape and create a legal and diplomatic framework to hold nation-states accountable.

Framework for U.S.-Russian Cyber Negotiations

The concept of a bilateral U.S.-Russia cyber dialogue is not new. In 2013, President Barack Obama and President Vladimir Putin formed a working group to engage senior-level experts on cyber issues and develop concrete measures to address common threats (Morcos, 2021). This effort resulted in the world's first package of intergovernmental agreements on confidence-building measures in cyberspace and created a hotline to prevent cyber incidents from escalating into serious conflicts (Chernenko, 2021). However, in response to Russia's annexation of Crimea in 2014, this bilateral dialogue was suspended. Diplomatic tensions escalated after the U.S. authorities accused Russia of interfering in the 2016 presidential election.

Since the 2020 election, U.S.-Russian relations have worsened. The Biden administration called Russia a “safe haven” for cybercriminals (Rosenbaum, 2021), accusing hackers living in Russia as the source of the Colonial Pipeline ransomware attack. Biden also urged Putin to take action against ransomware activities originating from Russia.

Despite their significant differences, both Russia and the U.S. recognized they had to talk to each other to avoid uncontrolled escalation in cyberspace. The resulting June 2021 U.S.-Russian summit in Geneva restarted discussions to address the surge of ransomware attacks, preventing cyberattacks on critical infrastructure industries. Although both sides agreed that the talks were constructive, there were no diplomatic breakthroughs aside from agreeing to continued dialogues on strategic stability and cybersecurity.

While Russia and the U.S. understand the importance of resolving cybersecurity's pressing issues, they seem to diverge over what should be done and how international law could be applied (McConnell, Sharikov & Smekalova, 2017). With advances in technology transforming the future of warfare, the two sides are struggling to find a common language with which to discuss arms control efforts in an age with new arsenals of cyber weapons.

Moscow and Washington bear a unique responsibility to keep the peace and discourage the proliferation of cyberattacks. The challenge is to find a balance between cooperation and competition and compartmentalize the relationship more effectively than at present (Stent, 2020). Tangible progress will be elusive in establishing a stable and predictable relationship with Russia. To achieve this goal starts with small wins, making cooperation a habit, and ultimately taking on the most demanding tasks as trusted partners.

CONSEQUENCES AND IMPACT OF CYBERATTACKS

The stakes could not be higher. A report by Symantec concluded that “with each passing year, not only has the sheer volume of threats increased, but the threat landscape has become more diverse, with attackers working harder to discover new avenues of attack and cover their tracks while doing so” (Symantec, 2018). By 2023, it is projected that half of all data breaches globally will occur in the United States (Norton, 2018). Due to the vast number of targets and the amount of financial resources, personal data, and intellectual property worth stealing, a study by Specops found that the U.S. has experienced more than triple the number of significant cyberattacks over the last 14 years than any other country (Brasseur, 2020). The U.S. faced 156 attacks -- more than the United Kingdom, India, Germany, South Korea, Australia, Ukraine, and China combined (Brasseur, 2020).

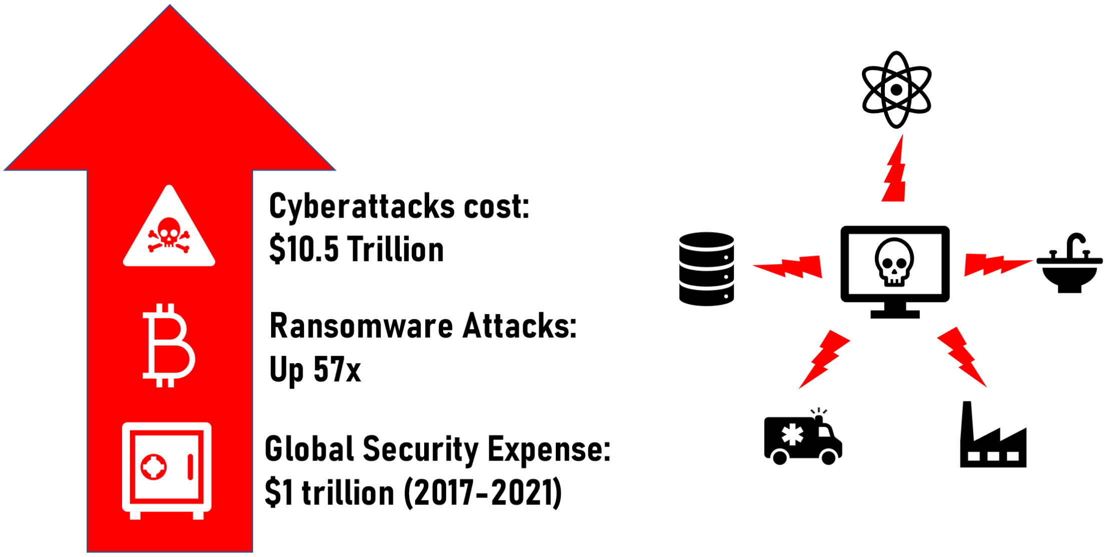
The starkest assessment came from a recent U.S. Naval War College report (Schneider, 2020) which warned:

> The growth of a global, interconnected cyberspace domain represents the biggest strategic development since 9/11. Activities and operations in, through, and from

> cyberspace now offer states the means to augment their power, degrade or usurp the power of others, and gain strategic advantage through competition without triggering armed conflict. Our adversaries have learned this and are leveraging it against us.

The Biden Administration's *Interim National Security Strategic Guidance* report recognized cybersecurity as a top priority (INSSG, 2020). Cyberattacks have emerged as among the most serious threats the U.S. faces. As highlighted in Figure 2 below, it is projected that cybercrime could cost the global economy $10.5 trillion annually by 2025 (Morgan, 2020). Damage from ransomware attacks is 57 times more than in 2015, and global spending on defending against cybercrime is estimated to exceed $1 trillion between 2017 to 2021 (Morgan, 2020).

Figure 2. Cyberattacks Cost and Impact



Source: *Morgan, S. "Cybercrime to Cost the World $10.5 Trillion Annually by 2025." Cybercrime Magazine, 13 Nov. 2020, cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.*

EVIDENCE ON POTENTIAL POLICY ALTERNATIVES

Several tentative conclusions and judgments emerge from the evidence at hand. First, cyber conflict has rapidly evolved and unfolded in unpredictable ways. Originally seen as an extension of state-on-state war, cyber operations were next perceived as an asymmetric tool for terrorists and small states to employ against critical infrastructure and then an all-powerful instrument of disinformation, social control, and coercion.

Second, all wars are now cyber wars as modern militaries and non-state actors supplement their conventional capabilities with cyber tactics. However, cyber conflict expands beyond the violent use of arms, becoming an indispensable tool in coercive diplomacy and strategic competition between states.

Third, since cyber operations can now cause strategic effects without the risks of war, states and non-states will seek their use more often, whether we respond or not. Operations below the use-of-force threshold may be just as effective and less risky than open war.

Preserving a secure internet depends on a shared understanding of norms, protocols, and standards. U.S. diplomatic efforts of naming and shaming, sanctions, and indictments, have insufficiently altered Russia's cost/risk calculus. Employing enforcement tools, including cyber case law,[3] attribution capability, confidence-building measures, and investments in hardening our critical infrastructure, will impose greater costs and encourage responsible state behavior among our adversaries.

Policy Alternative #1 - Developing & Defining Cyber Norms

Norms create expectations about behavior that make it possible to hold states accountable. Norms also help legitimize actions and help states recruit allies when they respond to a violation. In addition, norms can deter actions by imposing reputational costs that can damage an actor's soft power beyond the value gained from a given attack (Nye, 2017a).

For two decades, the U.S. and Russia have firmly opposed each other's U.N. cyber proposals. Whereas Washington wants to ensure the internet remains free and open to all, Moscow wants states to control the flow of information and those who may access it. Some experts have argued that one size does not fit all in cyberspace (Nye, 2022), and some norms may have to accommodate both authoritarian and democratic states and serve as a foundation for multilateral agreement.

As a senior State Department representative noted, "What we are doing is to lean into setting norms, standards and rules of the road for cyberspace through the U.N. and other international bodies" (Ignatius, 2021). In October, the U.S. and Russia achieved what many thought was unthinkable: They co-signed a cyber norms agreement (United Nations, 2021). The three-page document submitted to the U.N. General Assembly outlined, for the first time, general cyber principles on which the countries nominally agree. In essence, Moscow and Washington agreed to identify a common set of standards to prevent malicious cyberattacks. The two nations sharply differ about those standards, but in principle, there appears to be a shared commitment to cybersecurity.

The U.S. should pursue a parallel track with its allies to maintain momentum and diplomatic pressure. Initiatives such as the Global Commission on the Stability of Cyberspace (McConnell

[3] See Hollis, who notes that "international law does not have tailor-made rules for regulating cyberspace" and that "the current discourse centers not on whether international law applies, but rather how it does so" (Hollis, 2021).

et al., 2017), the 2017 G7 Declaration on Responsible States Behaviour in Cyberspace, and the 2019 Paris Call for Trust and Security in Cyberspace, are just a few efforts the U.S. can leverage to establish norms favorable to its national interests. These groups of democracies can set standards related to privacy, surveillance, and free expression and enforce them through special trade agreements. Experts note that if the U.S. and its allies can agree on cyber norms, "they are likely to be more willing to support imposing costs on violators, thus substantially improving the credibility, severity (through multilateral cost imposition), and sustainability of U.S. threats to impose costs in response to violations" (Nye, 2022).

Policy Alternative #2 – Banning Cyberattacks on Critical Infrastructure

Closely linked with establishing norms of behavior includes the protection of critical infrastructure from cyberattacks. When dealing with a Russian government that possesses an all-encompassing and conspiratorial view of the internet and regime security, the U.S. will have a better chance at successful cyber negotiations by narrowing its discussions to focus on defining the specific behaviors, targets, and costs in attacking them (Sherman, 2021).

This policy alternative aligns with the U.S. view that the internationally recognized laws of armed conflict (LOAC) that prohibit deliberate attacks on civilians apply in cyberspace. Accordingly, the United States would propose a ban on targeting certain civilian facilities in peacetime: "A state should not conduct or knowingly support online activity that intentionally damages critical infrastructure or otherwise impairs the use of critical infrastructure to provide services to the public" (Nye, 2017b). This is not a pledge of no first use of cyber weapons but of no use of cyber instruments against civilian facilities in peacetime.

During the Geneva Summit, Biden demanded that critical infrastructure should not be attacked and gave the Russian delegation a list of sixteen sectors[4] defined as "critical" (Biden, 2021a). The U.S. would also pursue a consultative process with Russia to establish a warning and negotiating framework, the most important ones being a mandate to provide states with assistance when requested and prohibitions against interfering with computer emergency response teams and allowing one's territory to be used for wrongful acts (Nye, 2022). In addition, the federal government would allocate financial and technical resources to harden our infrastructure to increase the cost of attack, further dissuading Russia and other non-state actors

[4] The Cybersecurity & Infrastructure Security Agency (CISA) defines 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety. These include the following sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials and waste; transportation systems; waste and wastewater systems. https://www.cisa.gov/critical-infrastructure-sectors

from targeting these sites. Coupled with strong deterrent threats, this process would seek to reduce the frequency and intensity of attacks from Russia.

Policy Alternative #3 - Cooperation Against Cybercrime

This policy alternative envisions a multi-pronged approach of engagement, information sharing, and enforcement for Moscow and Washington in taking the first steps in cooperating to investigate and prosecute cybercriminals.

First, the new Counter-Ransomware Initiative, announced by President Biden in October (Biden, 2021b), invited thirty countries to strengthen cooperation against ransomware and tackle the misuse of cryptocurrencies. The U.S. would include Russia in this multilateral initiative. Moscow will have more incentives to cooperate in fighting ransomware if the initiative is framed as a joint effort to face a common challenge rather than a U.S.-led coalition that considers Russia part of the problem. Having Russia as part of the collective effort on ransomware will not bridge all the differences. It will, however, shape a better understanding of what is possible in practice and help build much-needed trust for future talks (Shakirov, 2021). It not only creates buy-in on the part of Russia but accountability as well.

Second, Russian and American law enforcement agencies would also work out the mechanisms to jointly investigate cyber incidents, prosecute cybercriminals assist each other in damage control, and share information about international cyberthreats (McConnell et al., 2017). NGOs, civil society organizations, and public diplomacy institutions can work together to track and share information about criminal activities on the net with intelligence agencies. Creating a joint database of incidents would serve as a logical step in this direction (McConnell et al., 2017).

Third, and most importantly, the U.S. and its allies would create an independent agency similar to the International Atomic Energy Agency (IAEA) to determine attribution and monitor compliance (Williams, 2021). Creating an international standards body would set the minimum thresholds and technical standards for attribution. These standards would bolster both governments' ability to attribute cyber incidents using open-source information without exposing or jeopardizing their sources or methods (Zabierek et al., 2021). The attribution process would become transparent and conclusive by agreeing on such thresholds and standards.

CRITERIA FOR EVALUATING THE POLICY ALTERNATIVES

The following criteria were used to evaluate the different policy options.

- **Transparency:** Assess the coordination between Russia and the U.S. in identifying sources of cyberattacks. I will use a relative scale to measure the likelihood of increased transparency:
    - **Low** – anticipated to result in minimal transparency.
    - **Medium -** anticipated to increase transparency.

  - **High -** anticipated to achieve full transparency.

- **Security:** Assess the reduction in the number of successful attacks on critical infrastructure targets. I will use a relative scale to measure the likelihood of increased security:
  - **Low** – anticipated to achieve a small reduction in cyberattacks on one or more critical infrastructure targets.
  - **Medium -** anticipated to achieve a measurable reduction in cyberattacks on one or more critical infrastructure targets.
  - **High -** anticipated to achieve a significant reduction in cyberattacks on one or more critical infrastructure targets.
- **Accountability:** Assess the number of hackers identified, financial losses reduced, cases prosecuted, and criminals sent to prison. I will use a relative scale to measure the likelihood of increased accountability:
  - **Low** – anticipated to result in marginal improvements in jointly identifying hackers, reducing financial losses, and indicting criminals, but not resulting in any additional prosecutions or extraditions.
  - **Medium -** anticipated to achieve a measurable increase (5% or greater) in the number of hackers identified and cases prosecuted, a measurable decrease (5% or greater) in financial losses due to U.S.-Russian cooperation.
  - **High -** anticipated to achieve a substantive increase (10% or greater) in the number of hackers identified, cases prosecuted, and criminals sentenced, and a measurable decrease (10% or greater) in financial losses due to U.S.-Russian cooperation.

- **Cost:** Assess the financial costs for the U.S. to implement each option. I will use a relative scale to measure costs:
  - **Low** – marginal anticipated costs.
  - **Medium** – significant anticipated costs.
  - **High** – substantial and ongoing anticipated costs.

- **Political Viability:** Assess the likelihood that the U.S. and Russia will reach a bilateral agreement on the policy. I will use a relative scale to measure the likelihood of reaching a negotiated agreement:
  - **Low** – unlikely to achieve a negotiated agreement.
  - **Medium** – likely to achieve a negotiated agreement on at least one area of common interest or concern.
  - **High -** anticipated to achieve a negotiated agreement on multiple areas of common interest or concern.

Evaluation of Policy Alternative #1 - Developing & Defining Cyber Norms

In diplomacy, norms serve as the basis for transparency, mutual understanding, and shared expectations of behavior. Norms are critical in developing a theoretical framework for negotiation, defining and codifying principles, and influencing behavior.

***Transparency**:* Defining norms will also include intergovernmental agreements on confidence-building measures in the information space, such as a cyber hotline to prevent the threat of cyber incidents escalating into serious conflicts. In addition, several channels for the exchange of information can be established, including dialogue between the two nation's computer incident response centers. On the criterion of transparency, norms are **low**. While they clarify standards of behavior and could increase the levels of communication between the Kremlin and the White House, they do not reveal sources of cyberattacks.

***Security**:* On the criterion of security, norms are **low** because they rely upon Russian self-regulation not to launch an attack. Norms can deter actions by imposing reputational costs that can damage an actor's soft power beyond the value gained from a given attack (Nye, 2017a). However, Russia does not appear to place a high value on reputational risk, as seen by their recent invasion of Ukraine and the war crimes committed in Bucha, Irpol, and Mariupol.

***Accountability**:* Norms create expectations about behavior that make it possible to hold states accountable. Norms also help legitimize actions and help states recruit allies when they respond to a violation. However, norms are **low** on the criterion of accountability because they rely on each party's good faith and self-policing efforts to ensure compliance. Norms do not provide any enforcement mechanisms and therefore are limited in holding individual actors and nation-states accountable.

***Cost**:* On the criterion of costs, norms are **low** because they do not require financial resources from the federal government to deploy outside of the negotiation process. Norms are less flashy and less expensive than developing sophisticated cyberdefense systems but can reduce the number of attacks and financial losses as nations adhere to them.

Political Viability: On the criterion of political viability, norms are **high** because they will only apply during peacetime and are based on their previous commitments. Using the 2021 UN commitment as a baseline, the two adversaries could set limits on certain types of civilian targets and negotiate norms that minimize conflict. For example, the U.S. and Russia might negotiate limits on their behavior regarding each other's domestic political processes or targeting hospitals, electric grids, and other critical infrastructure (see Policy Alternative 2 below). Even without an agreement on precise definitions, they could announce unilateral statements about areas of self-restraint and establish a consultative process to contain conflict and mitigate escalation (Nye, 2019). By agreeing to these norms, Russia also receives public and diplomatic benefits to be seen as a rational actor in this sphere.

Evaluation of Policy Option #2 – Banning Cyberattacks on Critical Infrastructure

If the U.S. and Russia could agree on prohibiting attacks on critical infrastructure during peacetime, this would establish a precedent that would benefit the world. Convincing Russia that this would be in their self-interest requires exceptional diplomatic expertise, but the U.S. has the moral high ground due to Russia's invasion of Ukraine, and a united NATO and its Western allies by its side. Moreover, the U.S. possesses the most advanced technological capabilities and access to the deepest reservoir of financial assets and technical resources – both public and private – to harden its infrastructure from attack.

Transparency: On the criterion of transparency, banning cyberattacks on critical infrastructure is **medium** because neither the U.S. nor Russia have effectively addressed the issue of attribution regarding the source of cyberattacks. However, establishing formal deconfliction, verification, and inspection mechanisms, could take cues from previous arms control treaties. Cyberattacks manifest themselves in a real and physical form, from servers, routers, data storage facilities, cloud infrastructure, and the buildings where cyber operators work. Such measures as the joint investigation of IP addresses, disabling malware, securing data from internet service providers, identifying botnets, and other technical measures might be envisioned to increase transparency (Papp, 2019).

Security: On the criterion of security, this policy option is **high** because Russia and the U.S. have a mutual self-interest in declaring critical infrastructure off-limits to cyberattacks. Similar to the nuclear deterrence theory, the threat of retaliation remains a crucial tactic for preventing cyberattacks. Deterrence appears to be working since there have been no attacks on U.S. electrical systems to date, despite the reported Russian presence on the grid (Nye, 2019).

Accountability: On the criterion of accountability, this policy option is **medium** since denial by defense is effective in deterring non-state actors but less likely to prevent attacks by more powerful and proficient nation-state actors. Until the methods and means are developed to efficiently identify the source of the attack, combining the threat of punishment with an effective defense is the primary means to influence these powers' calculations of costs and benefits (Nye, 2022). Above all, the goal of this policy must be to avoid the rapid escalation of misunderstandings that could lead to reprisals or even armed conflict (Papp, 2019).

Cost: On the criterion of costs, protecting critical infrastructure is **high**. Investment in technological defenses and technical assistance to prevent cyberattacks is estimated to be $17.4 billion based on the most recent federal budget request, a $790 million (5 percent) increase above the FY 2019 estimate (Morgan, 2020). As technology advances, hardening our critical infrastructure against attacks and ensuring its prompt recovery will remain a costly long-term investment for both the public and private sectors.

Political Viability: On the criterion of political viability, this policy option is **medium** because Russia has expressed a willingness to discuss protecting critical infrastructure in peacetime. In advance of the 2018 Helsinki Summit, the Kremlin proposed cooperating with the United States to prevent "cyberattacks on critical infrastructure" (Grigsby, 2018). In addition, the March

2021 U.N. consensus report on cybersecurity, backed by both Washington and Moscow, re-affirmed that the two sides are committed to this goal (Zabierek et al., 2021).

Evaluation of Policy Alternative #3 - Cooperation Against Cybercrime

Although the U.S. is by far the largest target of cybercriminals, Russia is equally vulnerable to ransomware attacks, the loss of trade secrets, and outright theft. This fall, Russian financial organizations were hit by a record number of cyberattacks (Interfax, 2021), and Russian tech giant Yandex claimed it repelled the largest recorded DDoS attack ever (Reuter, 2021). Since it invaded Ukraine, Russia has experienced thousands of distributed denial of service attacks by amateur and professional hacktivists (Collier, Dong & Arouzi, 2022). The international cyber activist group, Anonymous, declared that it "was officially in cyber war" against Russia and is feeding the troves of data they hacked from the Russian Ministry of Defense, its Federal Security Service, and Russian state television (Halpern, 2022) to Distributed Denial of Secrets to release in the public domain (Gallagher, 2022). The onslaught of these attacks could incentivize Russia to seek U.S. assistance in addressing cybercrime.

Transparency: On the criterion of transparency, cooperation against cybercrime is **medium** because Moscow is unlikely to disclose or alert Washington if it infiltrates an infrastructure target, but it may be more willing to assist in identifying independent actors and cybercriminals provided the U.S. responds in kind. Because the U.S. initiative seeks to go after ransomware financing, Russia's track record of cooperating to combat money laundering and the financing of terrorism will be relevant. Russia is a member of the Financial Action Task Force and the Council of Europe's MONEYVAL, which seek to counter these criminal activities.
A 2019 evaluation of Russia's actions in this field cited "excellent use" of its financial intelligence in investigations (FATF, 2019).

Security: On the criterion of security, this policy option is **medium** because Russia faces a dramatic increase in the number of cyberattacks and, prior to the war in Ukraine, appeared open to negotiation on a broader range of cyber issues with Washington. These latest hacks and attacks by cybercriminals and activists have compromised Russian financial, communications, and military systems, placing its economy and national security at risk. Washington should expect a more favorable response from Moscow in addressing this issue once the Ukraine war concludes.

Accountability: On the criterion of accountability, if successfully implemented, this policy option is **medium** because eliminating safe havens for criminals is vital to stemming the tide of cyberattacks, and host nations must be held responsible. To achieve this objective requires improved technical resources to attribute the source of the cyberattack definitively, which currently do not exist.[5] Furthermore, if the criminals are identified, verification is required that the host nation has shut down the source and prosecuted those malign actors ensuring state-sponsored cyberunits cannot act with impunity (Carmack, 2021; Muir, 2014; Reuters, 2018).

Cost: On the criterion of costs, this policy option is **high**. Global spending on cybersecurity services to defend against cybercrime is projected to exceed $1 trillion over the five-year period from 2017 to 2021 (Morgan, 2020). Using the IAEA as a point of comparison, the cost of creating a similarly structured entity to monitor and prevent cybercrime would be approximately $477 million annually, of which $200 million is provided by the U.S. government (Kerr et al., 2021). Including the approximately $12 million annual budget of the Financial Action Task Force, which combats global money laundering and terrorist financing (*FATF Annual Report 2020-2021*), along with additional resources for the FBI and international law enforcement to investigate cybercrime would add another $500 million per year.

Political Viability: On the criterion of political viability, this policy option is **low** because Russia has not delivered on curbing ransomware attacks by criminals operating within its borders. President Biden raised the issue during a July 2021 phone call with Putin, warning of digital retaliation if Russia did not cooperate and cyberattacks continued (Holland & Shalal, 2021). Moscow agreed to form an expert group to assess the threat, but FBI Deputy Director Paul Abbate said he has seen “no indication” that Russia has gone after ransomware actors (Shakirov, 2021). Compounding matters, Russia’s cyber network comprises a complex web of state and independent actors, and many are in the gray area in between. Like its kleptocratic government structure, these groups can be state-backed, state-directed, state-encouraged, or state-ignored (Sherman, 2021). As a result, Russian officials consistently dismiss U.S. accusations of any wrongdoing in cyberspace. The biggest obstacle involves extraditing Russian criminals to the U.S. justice system to stand trial. This process would require reciprocity for U.S. criminals and is a non-starter for both nations.

Outcomes Matrix

As noted in Table 2, the matrix below provides a tabulated summary of the above analysis. In this matrix, low, medium, and high are used to show how effective the option is at achieving the goals of transparency, security, accountability, the relative costs of each option, and their political viability of execution.

Table 2. Outcomes Matrix

[5] Attributing the source of a cyberattack requires hiring an outside cybersecurity expert and often law enforcement agencies such as the FBI. Further complicating matters, hackers launch cyberattacks using computers or devices owned by other victims that the attacker has previously compromised. Identifying an attacker is made more difficult because attackers can use proxy servers to bounce their IP addresses around the world to confuse attempts at cyber attribution (Rosencrance 2017). Cyber attribution efforts are further hindered when attacks originate in nations that refuse to cooperate with U.S. law enforcement investigations.

Goals	**Impact**	**Policy 1: Developing & Defining Cybernorms**	**Policy 2: Protecting Critical Infrastructure**	**Policy 3: Cooperation Against Cybercrime**
Transparency	Increased coordination between Russia and the U.S. in identifying sources of cyberattacks.	Low	Medium	Medium
Security	Reduction in the number of successful Russian attacks on infrastructure targets.	Low	High	Medium
Accountability	Increased number of hackers identified, cases prosecuted, and criminals extradited to the U.S. or sent to prison, reduction of financial losses to U.S. entities.	Low	Medium	Medium
Cost	Financial costs for the U.S. to implement.	Low	High	High
Political Viability	Likelihood that the U.S. and Russia will endorse/execute the policy.	High	Medium	Low

RECOMMENDATION

Based on the projected outcomes of the analysis and the potential risks to our national security, I recommend that the United States pursue a ban on targeting critical infrastructure in peacetime. Although it is more costly than creating norms and may be less prevalent than cybercrime, the potential damage and lives at risk resulting from a malicious cyberattack on our electric grid, nuclear reactor, or communications systems are incalculable.

Both Russia and the U.S. have a mutual self-interest in declaring critical infrastructure off-limits to cyberattacks. The absence of a universal definition of unacceptable behavior against critical infrastructure that constitutes a legitimate *casus belli* between states leaves unclear the lines that, if crossed, could spiral into an international or military conflict (Van Epps, 2013). Worse, cyber has not only expanded the theater of war, but it has also expanded the number of rogue participants on the battlefield. Private cybercrime groups are taking sides and playing an active role in the Ukrainian war. Previously hackers focused on extracting ransom from companies. Many are now targeting the destruction of key infrastructure sites (Timu & Vilcu, 2022).

However, since they do not possess the same "war logic or frameworks" as nation-states (Timu et al., 2022), this raises the risk that their cyberattacks could spiral uncontrollably, causing significant collateral damage and loss of life. Although the ability to deter attacks by non-state actors is limited, the primary threat emanates from the Russian government, and that is where the U.S. has the greatest leverage.

The Russians also have much to lose in the cyber theater as the last "arms race" cost them dearly. Russia recognizes that the U.S. has a far greater reserve of resources and technical expertise to mobilize in this new arena. Moreover, President Biden has united NATO and our western allies in a way not seen since World War II. This alliance is a force multiplier in the cyber arena. These factors create an environment that should increase the likelihood of the U.S. and Russia reaching an agreement.

IMPLEMENTATION

Lessons from the Past – Not Unprecedented but Unlikely to Inform Today's Policy

During the height of the Cold War, Washington and Moscow managed to sign pivotal arms control agreements, including the multilateral 1963 Limited Test Ban Treaty, bilateral 1972 Anti-Ballistic Missile Treaty, Strategic Arms Limitation Talks Agreements (SALT I and SALT II), and the 1987 Intermediate-Range Nuclear Forces Treaty (Zabierek, 2021). The success of negotiating these treaties during that contentious era provides hope that some type of an agreement is possible.

One key distinction between those agreements and proposed deals for the cyber domain lies in verification. Compliance with arms treaties involves rigorous on-site inspections, information exchanges, and the ongoing monitoring of facilities (Zabierek, 2021). However, as Robert Papp, former director of the CIA's Center for Cyber Intelligence, observed, "Cyber verification is not the same as counting missiles, and inspection and confidence-building visits to cyber and signals intelligence facilities are unlikely ever to be envisioned or even relevant" (Papp, 2019). The U.S. and Russia must think more creatively about verification under any cyber agreements.

The Present – Uncertain, Undefined, Unknown

Russia's invasion of Ukraine has created the greatest diplomatic, political, military, and economic crisis since World War II. In a historic vote, the UN reprimanded Russia for its invasion of Ukraine (Pamuk et al., 2022), the UN Human Rights Council has begun an investigation into human rights violations and war crimes (Farge, 2022), while the Council of Europe has stripped Russia of its membership (COE, 2022). President Biden has recently ratcheted up his rhetoric accusing Putin of being a war criminal (Fossum & Liptak, 2022). Tensions between Moscow and Washington are the highest since the Cuban Missile Crisis. Advancing any negotiations on cybersecurity is non-existent until the war in Ukraine ends, and even then, Vladimir Putin and his regime are an international pariah, having lost all trust and credibility with the West.

How the war in Ukraine ends could have significant geopolitical consequences: scenarios range from Ukraine's capitulation, a long war of attrition and occupation, a military stalemate to Ukraine emerging victorious but at a tremendous financial and human cost. Worse, NATO and its allies could be drawn into the conflict, raising the prospect of World War III. Will Putin's hold on power remain and possibly be strengthened, such as what occurred in Chechnya, or will this invasion result in his political demise? Until then, U.S. foreign policy will remain focused on deploying every economic, humanitarian, military, and diplomatic tool against Putin, his political allies, and the Russian military.

Negotiating Terms & Conditions

If the U.S. and Russia restart negotiations, the following conditions must happen:

Bring all relevant stakeholders to the table.

The primary interlocutors would be representatives from the U.S. State Department and the Russian Ministry of Foreign Affairs. Since the issues involve offensive cyber actions against critical infrastructure, defining norms of behavior, formal deconfliction mechanisms, and potential cooperation on verification and inspection, officials from the Russian Security Council, Ministries of Defense, Internal Affairs, Federal Security Service, and Justice should be involved as part of a large interagency forum. On the U.S. side, this would include representatives from the U.S. Defense Department, Department of Homeland Security, Department of Justice, National Security Agency, the Office of the Director of National Intelligence, and the Cybersecurity & Infrastructure Security Agency.

Set clear and realistic expectations.

To the extent possible, the U.S. must leverage its diplomatic advantage and technological superiority to steer the agenda and set clear and realistic objectives. While Russia has few incentives to make significant concessions given the anonymous nature of cyberattacks, the Ukraine invasion has exposed the limits of Russia's military and cyber capabilities to the world. Russian networks have been routinely hacked and compromised, which should cause Moscow to rethink its hardline stance. However, the initial aim should not be to change Russia's behavior but to better understand its strategy, convey mutual concerns, and explore potential areas of cooperation (Morcos, 2021). A prime example would be prohibiting all cyber activities on each other's nuclear power facilities and nuclear weapons systems. This would include establishing norms not to attack nuclear communication, command, and control systems (Zabierek, 2021). Concurrently, the U.S. should explicitly communicate redlines and expectations for responsible behavior, particularly those activities considered to be an act of war or warrant retaliatory actions.

Allies are kept informed and engaged.

The Biden Administration's diplomatic efforts have united our European and NATO allies against Russia. While the negotiations are bilateral, the U.S. should brief its allies throughout the negotiations and leverage any public communication around the dialogue to its advantage. The U.S. should pursue a parallel track with its democratic partners to maintain momentum and diplomatic pressure. Initiatives such as the Global Commission on the Stability of Cyberspace (McConnell et al., 2017), the 2017 G7 Declaration on Responsible States Behaviour in Cyberspace, and the 2019 Paris Call for Trust and Security in Cyberspace, are just a few efforts the U.S. can leverage to establish terms favorable to its national interests. These groups can set privacy, surveillance, and free expression standards and enforce them through special trade agreements.

With the current war in Ukraine, the U.S. should put further diplomatic pressure on Russia by extending Article 5 of the NATO charter to include cyberattacks (Frydenborg, 2021). Amending Article 5 will put Russia on notice that any attack on a NATO nation will expand the cyber battleground resulting in an immediate response. Experts note that if the U.S. and its allies can agree on cyber norms, they can isolate rogue states such as Russia, and "they are likely to be more willing to support imposing costs on violators, thus substantially improving the credibility, severity (through multilateral cost imposition), and sustainability of U.S. threats (Nye, 2022).

While Russia and the U.S. may view cybersecurity differently, taking advantage of the commonalities that do exist is necessary to forge a broader agenda on cybersecurity. Finding common ground demands innovative partnering, breaking patterns of mistrust, and forging new means to identify and achieve common goals (Van Epps, 2013). In the context of U.S.–Russia relations, it will also require working through decidedly contradictory views and dissimilar cultures of security, and a track record lacking in sustained tangible cooperation (Sherr, 2011). There is a high demand for developing confidence and trust in bilateral relations to address the political contradictions between these nations. Both sides must be willing to take some risks to achieve appreciable results. Nevertheless, these risks are a modest investment that could offer a substantial return on cybersecurity issues of importance to all parties.

CONCLUSION

The need to ban attacks on critical infrastructure during peacetime is at a critical threshold. Recent reports indicate that Russia is preparing cyberattacks to disrupt U.S. energy and financial institutions in retaliation against U.S. sanctions (Detsch & Yang, 2022). President Biden has maintained a clear and consistent message to Vladimir Putin and Russia that any kinetic or cyber attack on critical infrastructure such as electricity, hospitals, and nuclear facilities and systems is off-limits. I would argue that the Biden administration raises the stakes that if Russia were to attack a U.S. or NATO ally's nuclear, energy, or chemical facility, this would be considered a war crime and that NATO would respond in kind.

Washington and Moscow recognize that they need to talk to each other despite their significant differences to avoid uncontrolled escalation in cyberspace. That is why even after the 2014 Russian invasion of Ukraine, the United States kept meeting with Russian cyber experts despite having cut cooperation elsewhere (Grigsby, 2018). With diplomatic relations suspended, dialogue on cybersecurity must happen outside of traditional institutions and networks. The U.S. should engage in Track 1.5 and Track 2 diplomacy[6] by communicating with Russian NGOs, academics, and other centers of influence to exchange information and concerns and foster goodwill. The U.S. should also exploit back channels and agents within the Russian government that support U.S. interests and have influence within the Russian leadership.

The attack on Ukraine has given the U.S. the diplomatic and moral high ground and united Western allies against Putin's autocratic regime. Russia's actions have reminded the world of the fragility of democracy and freedom. Washington must seize the moment and leverage its position with the support of its allies to define cyber norms, protect critical infrastructure, and bring cybercriminals to justice. The best of American foreign policy has been based on its ideals and when we approach matters for the collective good.

[6] Track 1 diplomacy is official government diplomacy involving heads of state and military leaders focusing on treaties and other agreements; Track 1.5 diplomacy includes official and non-official actors working together to resolve conflicts; Track 2 diplomacy is the unofficial intervention involving academic, NGO, and other non-state actors to build relationships and encourage new thinking that can inform the Track 1 process (Leguey-Feilleux. 2009).

BIBLIOGRAPHY

Annual Threat Assessment of the US Intelligence Community (ATA), 9 April, 2021, Office of the Director of National Intelligence, from https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*, *3*(4-5), 353–364. https://doi.org/10.1080/23340460.2017.1414924

Biden, J. R., (2021a, June 16). *Remarks by President Biden in Press Conference* [Press release]. Retrieved February 1, 2022, from https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/06/16/remarks-by-president-biden-in-press-conference-4/

Biden, J. R., (2021b, October 13). *Remarks by President Biden in Press Conference* [Press release]. Retrieved February 3, 2022, from https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/

Brasseur, K. (2020, July 13). *Study: U.S. largest target for 'significant' cyber-attacks*. Compliance Week. Retrieved November 30, 2021, from https://www.complianceweek.com/cybersecurity/study-us-largest-target-for-significant-cyber-attacks/29180.article.

Borghard, E., & Lonergan, S. (2017, May) "The Logic of Coercion in Cyberspace," Security Studies 26, no. 3 pp. 452–81.

Borghard, E., & Lonergan, S. (2018) "Confidence Building Measures for the Cyber Domain," Strategic Studies Quarterly 12, no. 3 (Fall 2018), pp. 10–49.

Bumiller, E., & Shanker, T. (2012, October 12). *Panetta warns of dire threat of cyberattack on U.S.* The New York Times. Retrieved November 30, 2021, from https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

Carmack, D. (2021). *Biden Administration Needs To Take the Kid Gloves Off When Reacting to China's Cyberattacks*. The Heritage Foundation. Retrieved October 20, 2021, from https://www.heritage.org/cybersecurity/commentary/biden-administration-needs-take-the-kid-gloves-when-reacting-chinas

CCDCOE. (2017). Ccdcoe.org. https://ccdcoe.org/news/2017/geneva-conventions-apply-to-cyberspace-no-need-for-a-digital-geneva-convention/

Chernenko, E. (2021, September 29). Axis Against Evil. Retrieved February 05, 2022, from https://www.kommersant.ru/doc/5007866

COE. (2022, March 18). The Russian Federation is excluded from the Council of Europe. Retrieved March 20, 2022, from https://www.coe.int/en/web/portal/-/the-russian-federation-is-excluded-from-the-council-of-europe

Collier, K., Dong, S., & Arouzi, A. (2022, March 22). Hackers around the World Deluge Russia's internet with simple, effective cyberattacks. NBC News. Retrieved April 6, 2022, from https://www.nbcnews.com/tech/security/hacktivists-new-veteran-target-russia-one-cybers-oldest-tools-rcna20652

Convention on Cybercrime. (n.d.). Impact of the European Convention on Human Rights. https://www.coe.int/en/web/impact-convention-human-rights/convention-on-cybercrime#/

Corn, (Col.) G. *International Law's Role in Combating Ransomware?* (2021, August 23). Just Security. https://www.justsecurity.org/77845/international-laws-role-in-combating-ransomware/

Detsch, J., & Yang, M. (2022, March 30). Russia prepares destructive cyberattacks. Foreign Policy. Retrieved April 6, 2022, from https://foreignpolicy.com/2022/03/30/russia-cyber-attacks-us-ukraine-biden/

Farge, E. (2022, March 04). UN Rights Body Approves Investigations into Alleged Russian Violations in Ukraine. Retrieved March 19, 2022, from https://www.reuters.com/world/un-rights-body-approves-probe-into-alleged-russian-violations-ukraine-2022-03-04/

FATF (2019), Anti-money laundering and counter-terrorist financing measures – Russian Federation, Fourth Round Mutual Evaluation Report, FATF, Paris http://www.fatf-gafi.org/publications/mutualevaluations/documents/russian-federation2019.html

FATF Annual Report 2020-2021 (p. 73, Rep.). (2021). Paris, France: Financial Action Task Force.

Fischerkeller, M. & Harknett, R. (2017). *Deterrence Is Not a Credible Strategy for Cyberspace*. Orbis 63, no. 1, pp. 381–93.

Ford, W. (2020, May 18). *The Cyberspace Solarium Commission Makes Its Case to Congress* [Review of *The Cyberspace Solarium Commission Makes Its Case to Congress*]. Lawfareblog.com; Lawfare. https://www.lawfareblog.com/cyberspace-solarium-commission-makes-its-case-congress

Fossum, S., & Liptak, K. (2022, March 17). Biden on Putin: 'I think he is a war criminal'. *CNN*. Retrieved April 6, 2022, from https://www.cnn.com/2022/03/16/politics/biden-calls-putin-a-war-criminal/index.html

Fruhlinger, J. (2017, August 22). *What is stuxnet, who created it and how does it work?* CSO Online. Retrieved November 30, 2021, from https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html.

Frydenborg, B. E. (2021, June 7). Already in a cyberwar with Russia, NATO must expand Article 5 to include cyberwarfare. Retrieved April 1, 2022, from https://realcontextnews.com/already-in-a-cyberwar-with-russia-nato-must-expand-article-5-to-include-cyberwarfare/?s=09

Gallagher, R. (2022, April 6). Distributed Denial of Secrets is Spreading Stolen Russian Data. Bloomberg. Retrieved April 6, 2022, from https://www.bloomberg.com/news/newsletters/2022-04-06/ddosecrets-group-helps-hackers-spread-russian-data

Goel, S. (2020). National Cyber Security Strategy and the Emergence of Strong Digital Borders. *Connections*, *19*(1), 73–86. https://www.jstor.org/stable/26934537

Goldsmith, J. (2011, February). *Cybersecurity Treaties: A Skeptical View* [Review of *Cybersecurity Treaties: A Skeptical View*]. http://www.futurechallengesessays.com; Hoover Institution. https://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf

Grigsby, A. (2018, August 27). Russia wants a deal with the United States on cyber issues. why does Washington Keep Saying No? Retrieved March 2, 2022, from https://www.cfr.org/blog/russia-wants-deal-united-states-cyber-issues-why-does-washington-keep-saying-no

Halpern, S. (2022, March 22). The threat of Russian cyberattacks looms large. The New Yorker. Retrieved April 6, 2022, from https://www.newyorker.com/news/daily-comment/the-threat-of-russian-cyberattacks-looms-large

Hayden, M. V. (2017). In *Playing to the edge: American intelligence in the age of terror* (pp. 151–152). Penguin Books.

The Heritage Foundation. (2019). *The Growing Threat of Cyberattacks*. The Heritage Foundation. https://www.heritage.org/cybersecurity/heritage-explains/the-growing-threat-cyberattacks

Holland, S., & Shalal, A. (2021, July 10). Biden presses Putin to act on ransomware attacks, hints at retaliation. Reuters. Retrieved February 05, 2022, from https://www.reuters.com/technology/biden-pressed-putin-call-act-ransomware-attacks-white-house-2021-07-09/

Hollis, D. (2021, June 14). *A brief primer on International Law and Cyberspace*. Carnegie Endowment for International Peace. Retrieved November 29, 2021, from https://

carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763.

Ignatius, D. (2021, October 19). The ice between the U.S. and Russia may be thawing - for now. Washington Post. Retrieved February 02, 2022, from https://www.washingtonpost.com/opinions/2021/10/19/ice-between-us-russia-may-be-thawing-now/

Interfax (2021, October 01). VTB recorded a sharp increase in cyber attacks in September. Retrieved February 05, 2022, from https://www.interfax.ru/business/794709

International Committee of the Red Cross (ICRC). (2014, January 1). *The Geneva Conventions of 1949 and their additional Protocols*. International Committee of the Red Cross. Retrieved November 30, 2021, from https://www.icrc.org/en/document/geneva-conventions-1949-additional-protocols.

International Law Commission. (2001). *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries 2001*. (n.d.). https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

Interim National Security Strategic Guidance (INSSG), The White House, 2021, p. 18.

International Strategy for Cyberspace, The White House, 2011, p. 13. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Ivan, P. (2019, March 18). *Responding to cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox* [Review of *Responding to cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox*]. European Policy Centre. https://epc.eu/en/publications/Responding-to-cyberattacks-EU-Cyber-Diplomacy-Toolbox~218414

Kreuzer, M. P. (2021, July 8). *Cyberspace is an analogy, not a domain: Rethinking domains and layers of warfare for the information age*. The Strategy Bridge. Retrieved November 27, 2021, from https://thestrategybridge.org/the-bridge/2021/7/8/cyberspace-is-an-analogy-not-a-domain-rethinking-domains-and-layers-of-warfare-for-the-information-age.

Lancelot, J. F. (2020). Cyber-diplomacy: cyberwarfare and the rules of engagement. *Journal of Cyber Security Technology*, 1–15. https://doi.org/10.1080/23742917.2020.1798155

Leguey-Feilleux, J. (2009). Libguides: SRS: 3.2 conference diplomacy. Retrieved March 20, 2022, from https://mcrl.libguides.com/SRS/Module3_2

Lewis, J. (2010, June). *Multilateral Agreements to Constrain Cyberconflict* [Review of *Multilateral Agreements to Constrain Cyberconflict*]. Arms Control Association. https://www.armscontrol.org/act/2010-06/multilateral-agreements-constrain-cyberconflict

Morgan, J. (2017, April 20). *A simple explanation of 'the internet of things'*. Forbes. Retrieved November 29, 2021, from https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/.

Market Business News. (2019, May 18). *What is first-mover advantage? definition and examples*. Market Business News. Retrieved November 30, 2021, from https://marketbusinessnews.com/financial-glossary/first-mover-advantage-definition-meaning/.

McConnell, B. W., Sharikov, P., & Smekalova, M. (2017, May). Suggestions on Russia-U.S. Cooperation in Cybersecurity. Russian Council. Retrieved February 4, 2022, from https://russiancouncil.ru/papers/RIAC-EWI-Russia-U.S.-Cybersecurity-Policybrief11-en.pdf

Morcos, P. (2021, July 13). Cyber dialogues with Russia: Lessons from France. *Center for Strategic & International Studies*. Retrieved February 07, 2022, from https://www.csis.org/analysis/cyber-dialogues-russia-lessons-france

Morgan, P. M. (2003). *Deterrence now. Cambridge Studies in International Relations 89. Cambridge [England]*. New York: Cambridge University Press.

Morgan, S. (2020, 13 Nov.) "Cybercrime to Cost the World $10.5 Trillion Annually by 2025." *Cybercrime Magazine*, from https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Muir, L. (2014). *Combatting Cyber-Attacks Through National Interest Diplomacy: Combatting Cyber-Attacks Through National Interest Diplomacy: A Trilateral Treaty with Teeth A Trilateral Treaty with Teeth*. Retrieved October 20, 2021, from https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=1005&context=wlulr-online

Nakasone, P. M. (2019, February 2). *A cyber force for persistent operations*. 459th Air Refueling Wing. Retrieved November 28, 2021, from https://www.459arw.afrc.af.mil/News/Article-Display/Article/1737519/a-cyber-force-for-persistent-operations/.

"NATO 2030. United for a new era": a Digest. (2020). JSTOR. http://www.jstor.org/stable/resrep27747

Norton. (2018). *10 cyber security facts and statistics for 2018*. Retrieved November 30, 2021, from https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html.

Nye, J. S., Jr. (2017a, January 01). Deterrence and Dissuasion in Cyberspace. Retrieved February 06, 2022, from https://direct.mit.edu/isec/article/41/3/44/12147/Deterrence-and-Dissuasion-in-Cyberspace

Nye, J. S., Jr. (2017b, May 5). Normative restraints on Cyber Conflict. Retrieved February 1, 2022, from https://sipa.columbia.edu/sites/default/files/ Nye_Normative_Restraints_on_Cyber_Conflict_0502.pdf

Nye, J. S., Jr. (2022, January 21). The End of Cyber-Anarchy? Retrieved February 02, 2022, from https://www.foreignaffairs.com/articles/world/2021-12-14/end-cyber-anarchy

Pamuk, H., & Landay, J. (2022, March 03). U.N. General Assembly in historic vote denounces Russia over Ukraine invasion. Retrieved March 18, 2022, from https://www.reuters.com/ world/un-general-assembly-set-censure-russia-over-ukraine-invasion-2022-03-02/

Papp, R. G. (2019, March). A Cyber Treaty with Russia. Retrieved February 16, 2022, *Wilson Center*, from https://www.wilsoncenter.org/sites/default/files/media/documents/ publication/kennan_cable_no._41.pdf

Reuters. (2018, November 9). U.S. accuses China of violating bilateral anti-hacking deal. *Reuters*. https://www.reuters.com/article/us-usa-china-cyber/u-s-accuses-china-of-violating-bilateral-anti-hacking-deal-idU.S.KCN1NE02E

Reuters. (2021, September 09). Russia's Yandex says it repelled biggest ddos attack in history. *Reuters.* Retrieved February 05, 2022, from https://www.reuters.com/technology/russias-yandex-says-it-repelled-biggest-ddos-attack-history-2021-09-09/

Robertson, J. (2022, March 16). Russian Isolation Spells Trouble for Global Cybersecurity. Retrieved March 16, 2022, from https://www.bloomberg.com/news/newsletters/ 2022-03-16/russian-isolation-spells-trouble-for-global-cybersecurity

Robinson, L., Migacheva, K., Magnuson, M., Radin, A., Nader, A., Cohen, R. S., & Helmus, T. C. (2019). *The Growing Need to Focus on Modern Political Warfare* (p. 2, Issue brief). Santa Monica, CA: RAND Corporation. doi:https://doi.org/10.7249/RB10071

Rosenbaum, E. (2021, May 26). Biden-Putin Summit Tensions: Feds say Russia a hacker 'safe haven'. CNBC. Retrieved February 03, 2022, from https://www.cnbc.com/2021/05/26/ darkside-will-be-back-as-russia-creates-safe-haven-for-hackers-feds.html

Rosencrance, L. (2017, October 31). *What is cyber attribution?* SearchSecurity. Retrieved November 30, 2021, from https://www.techtarget.com/searchsecurity/definition/cyber-attribution.

Runde, D., & Ramanujam, S. (2021, August 2). *Digital Governance: It Is Time for the United States to Lead Again* [Review of *Digital Governance: It Is Time for the United States to Lead Again*]. Center for Strategic & International Studies. https://www.csis.org/analysis/ digital-governance-it-time-united-states-lead-again

Schneider, J. et al. (2020). *Ten Years In: Implementing Strategic Approaches To Cyberspace*. Newport: U.S. Naval War College, December 2020. NATO similarly adopted this assumption in 2016, expanding the construct to all key U.S. allies. See Steve Evans. “Cyberspace is the New Domain for War: NATO.” in *Infosecurity Magazine*, June 16

2016. Accessed 11 November 2021 from https://www.infosecurity-magazine.com/news/cyberspace-is-new-domain-for-war/

Segal, A. (2016, September 16). *The U.S.-China Cyber Espionage Deal One Year Later* [Review of *The U.S.-China Cyber Espionage Deal One Year Later*]. Council on Foreign Relations. https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later

Shakirov, O. (2021, October 19). Why the United States Should Have Invited Russia to Join the Counter-Ransomware Initiative [Web log post]. Retrieved February 1, 2022, from https://www.cfr.org/blog/why-united-states-should-have-invited-russia-join-counter-ransomware-initiative

Sharma, I. (2021). Policy Recommendations. In *A More Responsible Digital Surveillance Future: Multi-stakeholder Perspectives and Cohesive State & Local, Federal, and International Actions* (pp. 32–44). Federation of American Scientists. http://www.jstor.org/stable/resrep30584.7

Sherman, J. (2021, November 11). The U.S. and Russia might finally be making a tiny bit of progress on cybersecurity. Slate.com. Retrieved February 01, 2022, from https://slate.com/technology/2021/11/russia-us-cyber-norms-agreement-general-assembly.html

Sherr, J. (2011, July 11). NATO and Russia: Doomed to Disappointment? *NATO*. Retrieved March 1, 2022, from https://www.nato.int/docu/review/articles/2011/07/11/nato-and-russia-doomed-to-disappointment/index.html

Significant cyber incidents. Significant Cyber Incidents | Center for Strategic and International Studies. (n.d.). Retrieved November 30, 2021, from https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

Singer, P. W. (2014). *Cybersecurity and Cyberwar: What everyone needs to know*. Oxford University Press, U.S.A.

Stent, A. (2020, April 27). Why are U.S.-Russia relations so challenging? Retrieved February 03, 2022, from https://www.brookings.edu/policy2020/votervital/why-are-us-russia-relations-so-challenging/

Symantec (2018). Internet Security Threat Report 23, p. 5. https://www.symantec.com/content/dam/symantec/docs/reports/ istr-23-2018-en.pdf

Taddeo, M. (2017, October 16). *The limits of deterrence theory in Cyberspace*. Philosophy & Technology. Retrieved November 30, 2021, from https://link.springer.com/article/10.1007/s13347-017-0290-2.

Tallinn Manual 2.0. (2017). Ccdcoe.org. https://ccdcoe.org/research/tallinn-manual/

Thomson Reuters. (2010, February 6). *Iran's police vow no tolerance towards protesters*. Reuters. Retrieved November 26, 2021, from https://www.reuters.com/article/us-iran-opposition-police/irans-police-vow-no-tolerance-towards-protesters-idU.S.TRE61511N20100206.

Timu, A., & Vilcu, I. (2022, April 4). Ukraine Crisis Tests Cyber Warfare's Red Lines, Bitdefender Says. Bloomberg. Retrieved April 6, 2022, from https://www.bloomberg.com/news/articles/2022-04-04/ukraine-clash-tests-red-lines-of-cyber-warfare-bitdefender-says

United Nations, General Assembly. (2021, October 8). *Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies* (First Committee ed., Vol. 66th Session, Agenda item 95). New York, NY: United Nations. N2128102.pdf (un.org)

U.S.MC. (n.d.) *Law of war/ introduction to rules of Engagement B130936 ...* United States Marine Corps. Retrieved November 30, 2021, from https://www.trngcmd.marines.mil/Portals/207/Docs/TBS/B130936%20Law%20of%20War%20and%20Rules%20Of%20Engagement.pdf.

Valeriano, B. (2015, January 15). *The Myth of the Cyber Offense: The Case for Restraint* (B. Jensen, Ed.) [Review of *The Myth of the Cyber Offense: The Case for Restraint*]. CATO Institute. https://www.cato.org/policy-analysis/myth-cyber-offense-case-restraint#cyber-command-s-new-more-aggressive-policy

Van Epps, G. (2013). Common Ground: U.S. and NATO Engagement with Russia in the Cyber Domain. *Connections*, *12*(4), 15–50. http://www.jstor.org/stable/26326340

Williams, B. "Meet the Scholar Challenging the Cyber Deterrence Paradigm," Fifth Domain, 19 July 2017, https://www.fifthdomain.com/.

Wittmann, V. (2020). DIGITAL DIPLOMACY VERSU.S. DOWNFALL. AN AGENDA FOR INTERNATIONAL RELATIONS IN THE GLOBAL AGE. *Русская политология – Russian Political Science*, *2(15)*. https://doi.org/10.51180/rps.2020.15.2.001

Zabierek, L., Lawrence, C., Neumann, M., & Sharikov, P. (2021, June 10). U.S.-Russian Contention in Cyberspace: Are Rules of the Road Necessary or Possible? Retrieved March 12, 2022, from https://russiamatters.org/analysis/us-russian-contention-cyberspace-are-rules-road-necessary-or-possible