RUSSIA MATTERS × THE CYBER PROJECT × IPNT

US-Russian Contention in Cyberspace

Are "Rules of the Road" Necessary or Possible?

AUTHORS:

Lauren Zabierek

Christie Lawrence

Miles Neumann

Pavel Sharikov

EDITORS:

Natasha Yefimova-Trilling

Simon Saradzhyan

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
JUNE 2021

Russia Matters
The Cyber Project
The U.S.-Russia Initiative to Prevent Nuclear Terrorism

Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.russiamatters.org
www.belfercenter.org/Cyber
www.belfercenter.org/USRIPNT

Design and layout by Andrew Facini

Printed in the United States of America

RUSSIA MATTERS × THE CYBER PROJECT × IPNT

US-Russian Contention in Cyberspace

Are "Rules of the Road" Necessary or Possible?

AUTHORS:

Lauren Zabierek

Christie Lawrence

Miles Neumann

Pavel Sharikov

EDITORS:

Natasha Yefimova-Trilling

Simon Saradzhyan

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
JUNE 2021

About the Authors

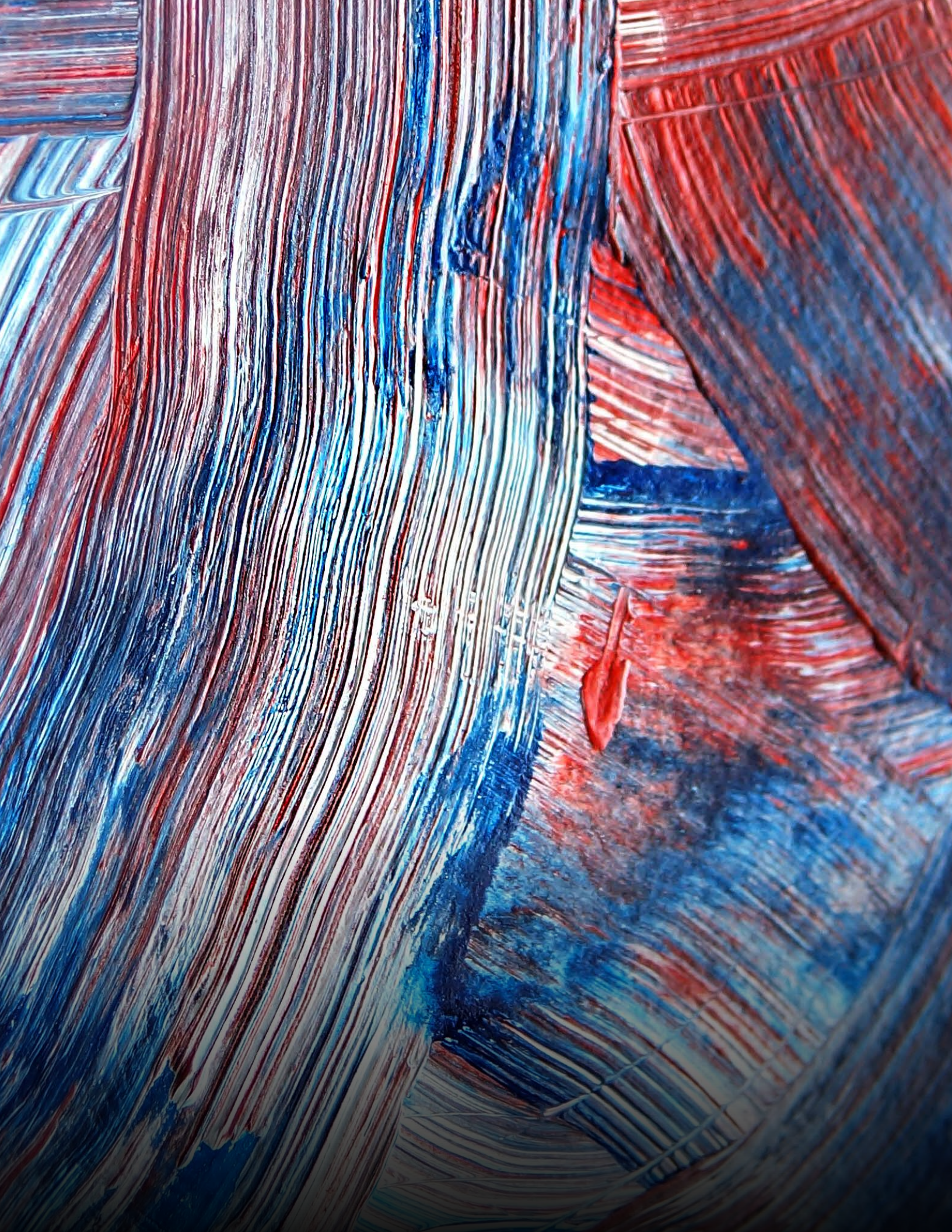
Lauren Zabierek is the executive director of the Cyber Project at Harvard Kennedy School's Belfer Center for Science and International Affairs. She is a former intelligence analyst and is also a co-founder of #ShareTheMicInCyber.

Christie Lawrence is a director for research and analysis at the National Security Commission on Artificial Intelligence. Prior to that position, she worked at the Belfer Center's Cyber Project and the State Department. She is a concurrent MPP/JD candidate at Harvard Kennedy School and Stanford Law School.

Miles Neumann is an investor focusing on cybersecurity, infrastructure software and developer tools at Insight Partners, a New York private equity firm. Before Insight, he was a researcher at the Belfer Center, working for Prof. Graham Allison and the Cyber Project.

Pavel Sharikov is a senior researcher at the Russian Academy of Sciences' Institute for U.S. and Canadian Studies (ISKRAN) and an associate professor at Moscow State University's School of World Politics. He was recently a visiting scholar at the University of Maryland's School of Public Policy.

Table of Contents



Introduction

By Natasha Yefimova-Trilling and Simon Saradzhyan

In recent years, as news of U.S.-Russian tensions in the cyber domain has dominated headlines, some strategic thinkers have pointed to the need for a bilateral cyber "rules of the road" agreement. American political scientist Joseph Nye, a former head of the U.S. National Intelligence Council, wrote in 2019 that, even "if traditional arms-control treaties are unworkable" in cyberspace, "it may still be possible to set limits on certain types of civilian targets, and to negotiate rough rules of the road that minimize conflict." Robert G. Papp, a former director of the CIA's Center for Cyber Intelligence, has likewise argued that "even a cyber treaty of limited duration with Russia would be a significant step forward." On the Russian side, President Vladimir Putin himself has called for "a bilateral intergovernmental agreement on preventing incidents in the information space," comparing it to the Soviet-American Agreement on the Prevention of Incidents on and Over the High Seas. Amid joint Russian-U.S. efforts, the Working Group on the Future of U.S.-Russia Relations recommended several elements of an agreement in 2016, among them that Russia and the U.S. agree "on the types of information that are to be shared in the event of a cyberattack" (akin to responses to a bio-weapons attack) and prohibit both "automatic retaliation in cases of cyberattacks" and "attacks on elements of another nation's core internet infrastructure." Most recently, in June 2021, a group of U.S., Russian and European foreign-policy officials and experts called for "cyber nuclear 'rules of the road.'"

Hearing some of these calls, we at Russia Matters and the U.S.-Russia Initiative to Prevent Nuclear Terrorism were moved to probe them further: Is a cyber rules-of-the-road agreement feasible? If so, what form could it take? If not, what are some next-best alternatives? We proceeded to formulate research questions (see Appendix 2) and seek out authors who could separately explore the American and the Russian perspectives on the cyber-treaty idea. The two research teams did not communicate with one another during the writing process;

this approach was chosen in order to juxtapose the two sides' viewpoints as starkly as possible, identifying and highlighting salient differences as well as areas for potential cooperation. While the authors are all affiliated with different institutions, they have written this paper in their personal capacity, representing the views of neither their organizations nor their governments.

Below we outline points on which the authors agree, disagree or cover ground that their counterparts did not. The overarching question imparting urgency to this exploration is: Can U.S.-Russian contention in cyberspace cause the two nuclear superpowers to stumble into war? In considering this question we were constantly reminded of recent comments by a prominent U.S. arms control expert: At least as dangerous as the risk of an actual cyberattack, he observed, is cyber operations' "blurring of the line between peace and war." Or, as Nye wrote, "in the cyber realm, the difference between a weapon and a non-weapon may come down to a single line of code, or simply the intent of a computer program's user."

Points on which the Russian and U.S. authors agree:

- While a formal, binding bilateral agreement is not possible now due to mutual mistrust, misunderstanding and stark differences in approaches to the cyber domain, necessary steps by Moscow and Washington include bilateral engagement, Track 2 and/or 1.5 dialogues and well thought-out confidence-building measures.
- The U.S. and Russia should strive toward a much better understanding of one another's red lines (i.e., what actions would trigger retaliation, especially kinetic retaliation) and cyber-mission priorities, intents, capabilities and organization.
- The U.S. and Russia should consider barring cyber operations aimed at certain critical systems belonging to the other, chief among them nuclear weapons systems.
- Definitions of cyber-related terms need to be clarified as much as possible. (Currently, ambiguity can be problematic even within a single language, much less across languages; the term "cyberattack,"

for example, is widely used in English-language news media and everyday speech to mean any sort of breach of cyber systems, while the U.S. military defines a "cyberspace attack" more narrowly.)

- The distinction between cyber defense and cyber offense can be elusive.
- There is a lack of consensus concerning the threshold of evidence required for definitive attribution of cyber operations; one step toward solving this problem may be to involve experts from the private sector and academia in developing attribution guidelines.
- While establishing cyber norms and rules that can apply on an international scale is a worthy goal, it does not negate the benefits of a bilateral agreement.
- Both the U.S. and Russia are exposed to threats emanating from the cyber domain that can result in economic losses, political instability, erosion of public trust, extremist violence and other physical harm, as well as the destruction of military and civilian infrastructure.
- Both the U.S. and Russia view misinformation and disinformation disseminated by cyber means as highly problematic.
- The Russian government tries to maintain greater control over domestic cyberspace than does the U.S., primarily to ensure political stability.
- At some point the U.S. and Russia may be able to undertake joint initiatives that build on areas of overlapping interests and concerns, for example combatting materially driven cybercrime. (NB: The U.S. authors are more skeptical about such efforts than the Russian author.)
- If ever a cyber rules-of-the-road agreement is signed, the U.S. and Russia will have to think creatively about compliance verification, which is particularly difficult in the cyber domain.

Points on which the Russian and U.S. authors disagree:

- While the Russian author believes that a risk of cyber-related escalation to kinetic conflict between Russia and the U.S. does exist (for instance, in the event of a cyber breach of the other side's weapons systems), the U.S. authors are hesitant to affirm the likelihood of such escalation as there have not yet been significant real-world examples of it and, more generally, the risks are still underexplored. (At least one study has concluded that great-power cyber competition in the 21st century does not "create new escalation risks.") Instead, the U.S. authors consider the greater risk to come from unintended, or intended, destruction or catastrophic damage resulting from malware.

- While the Russian author believes the U.S. should "be more open to dialogue without preconditions," the American authors call for "codified procedures for negotiations," with a "clearly defined timeline and set list of topics," as one of the conditions for moving toward a bilateral cyber agreement. Moreover, the U.S. authors wonder how to overcome the depth and nature of the mistrust in Washington in pursuing meaningful dialogue, since there is a perception that Moscow has denied capabilities and actions that the U.S. considers to be well established.

- While the U.S. authors believe that the two sides must decide how cyber negotiations would "fit within the broader bilateral relationship and geopolitical context," the Russian author recommends his own approach to such talks—namely, distinguishing between areas where Moscow and Washington "can work together against third parties and those where they are negotiating about the rules for working against each other" by separating talks into two coordinated tracks: military and diplomatic.

- The authors likewise have differing assessments of cyber-related progress on the diplomatic front: While the Russian author describes "impressive successes" in bringing the U.S. and Russian positions on cybersecurity closer together at the U.N., most notably with a consensus report on norms of responsible behavior by states

in March 2021, the U.S. authors note that Russia has used multilateral institutions, including two U.N. groups on cybersecurity, "to advance its own conceptualization of cyber norms, sometimes undermining Western influence."

- Finally, as noted above, the U.S. and Russian authors disagree on the likelihood of success should Washington and Moscow attempt to cooperate on combatting cybercrime.

Points on which the respective authors cover ground that their counterparts do not:

- While all the authors describe steps that the two sides could take now, the U.S. authors devote considerable attention to five prerequisites they consider necessary for the start of future talks on bilateral cyber rules of the road: codified procedural norms (as noted above), the appropriate rank of participants on both sides, clear attribution standards, a mutual understanding of proportional retaliatory actions and "costly signaling."
- The Russian author believes that Moscow must agree to discuss cyber-related topics in a military context. (Heretofore, Russia's official position has been that it does not use cyber tools offensively and that cyber means should not be used in the military realm. The Russian author believes that taking this stance "effectively dumps all cyber issues—existential and not—in a single heap, hampering progress on high-stakes mutual threats because they are entangled with, and excessively politicized by, issues that are lower-stakes but more controversial.")
- The Russian author likewise believes the U.S. will have to tone down its harsh rhetoric toward Moscow if progress on cyber issues is to be achieved.
- The U.S. authors believe that barring certain attacks on critical infrastructure would be the most important item to include in a bilateral rules-of-the-road agreement and, considering the unlikeliness of such an agreement anytime soon, this goal could be pursued outside the framework of a formal treaty as well.

- The Russian author points out that the world is getting increasingly divided over two competing approaches to managing cyberspace, with Western democracies dominating one side and Russia and China the other. By tallying several key indices for countries cosponsoring competing cyber-related resolutions proposed by Russia and the U.S. at the United Nations in 2018 and 2020, he demonstrates that the countries on Russia's side are "much less technologically advanced and politically less integrated into the digital world" than those on the U.S. side: "There seems to be a clear borderline between the nations that pursue strong government control similar to Russia's 'sovereign internet' or China's 'Great Firewall' and those that promote freedom of speech and a more democratic internet."

- If the goal of concluding a U.S.-Russian cyber treaty were to become more realistic, the U.S. authors conclude that buy-in from the U.S. legislative branch would be crucial and rules that narrowly focus on technical infrastructure—for example, forbidding illicit changes to ballots or hacks of election software and hardware—may be the most palatable for both sides, as opposed to broader, more general rules.

- The U.S. authors believe that key concerns for the U.S. government in the cyber domain include stopping foreign interference and disinformation intended to undermine American democracy, protecting critical infrastructure, preventing or guarding against reckless malware and safeguarding confidential communications, and that some of the related threats emanate "directly from Russia." One of Moscow's chief interests, in the U.S. authors' view, is "weaponizing cyber capabilities to sow discord and embarrass Western powers it views as undermining its sovereignty (principally the United States)."

- The Russian author does not speculate on national interests per se but does describe major cyber-related disagreements between Russia and the U.S. in at least three major areas: the role of government in overseeing cyberspace; the militarization of cyberspace and the related applicability of existing international law; and the idea of legally binding treaties versus non-binding guidelines for how information and communication technologies should be used.

Prospects for US-Russia Cyber Rules of the Road: An American Perspective

By Lauren Zabierek, Christie Lawrence and Miles Neumann

In 2020-2021 the United States found itself unraveling one of the largest cyber espionage operations in history. From what we knew early on, the campaign targeted U.S. civilian critical infrastructure and U.S government networks and was most likely perpetrated by actors associated with the Russian intelligence community, an accusation Russian officials have repeatedly denied. While we may never fully know the scope of the perpetrators' access to and theft of sensitive information, executed via trojanized software updates from the firm SolarWinds, the damage to our national security is grave. In its magnitude and scale, this breach offers the opportunity to analyze real-world activities against the backdrop of what has heretofore been a drawn-out and nebulous debate over norms. The United States should recognize this as the moment to declare what it considers appropriate and not appropriate in cyberspace so that we can prevent catastrophic damage at home and worldwide.

In the aftermath of the SolarWinds breach many have asked, "Was this operation an act of war?" Some have even described it as the "cyber equivalent of Pearl Harbor," which we believe is hyperbolic and offers the wrong analogy. The confusion at least partly stems from the lack of clarity around what specific cyber actions constitute an armed attack or act of war: For example, former Undersecretary of Defense for Intelligence Marcel Lettre once wrote that "cyberattacks that proximately result in significant loss of life, injury, destruction of critical infrastructure or serious economic impact" could be assessed as an "act of war" on a case-by-case basis. In layman's terms—and based on a definition of cyberattacks in the

NATO-commissioned Tallinn Manual 2.0[1]—the SolarWinds operation was not an act of war, at least not at this point in our understanding of its impact and intent.

We do believe, however, that the breach went beyond traditional espionage, as it targeted civilian infrastructure, private companies and networks and gave the perpetrators the potential ability to damage or destroy them, as well as federal entities' networks and infrastructure (and potentially to cause further harm to civilian populations). Such a move has been referred to as "holding targets at risk," which seems particularly dangerous upon examination of other Russian operations that demonstrated similar target reconnaissance and preparation. Furthermore, if the investigation of the SolarWinds operation unearths destructive malware, we may choose to update our assessment: In the words of the first Tallinn Manual, "the introduction of malware or production-level defects that are either time-delayed or activate on the occurrence of a particular event is an attack when the intended consequences meet the requisite threshold of harm." In any case, the breach lays bare the animosity between the U.S. and Russia that has festered within the foreign policy, national security and intelligence communities for years. Russia's alleged cyber activities in the past year or so alone include stealing highly sensitive information, sowing distrust and targeting U.S. critical infrastructure, and there is no evidence to suggest that such activity will cease anytime soon.

Even as the Biden administration enacts sanctions and other diplomatic and financial actions against Russia in response to the SolarWinds

1 The Tallinn Manual was developed by a group of experts convened by NATO and seeks to apply the Law of Armed Conflict (LOAC) to cyber warfare. LOAC refers to a body of international law that governs "armed conflict" between states and armed groups; its goal is to reduce suffering, loss and damage caused by violent conflict. LOAC does not refer to one specific law but instead derives from customary international law and treaty law, in particular the four 1949 Geneva Conventions, the 1977 additional Protocols to the Geneva Conventions and various other conventions with restrictions on acceptable weapons or conduct. The first Tallinn Manual, published in 2013, argued that "long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace."

The Tallinn Manual 2.0, an update issued in 2017, sought to apply international law to cyber incidents both in and outside of armed conflict, or incidents that fell below the threshold of war. Neither of the two versions is legally binding. The Tallinn Manual 2.0 provides some helpful definitions but did not clearly define what would constitute an act of war: "A cyberattack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction of objects… The notion of 'attack' is a concept that serves as the basis for a number of specific limitations and prohibitions in the law of armed conflict. For instance, civilians and civilian objects may not be 'attacked' (Rule 32). This rule sets forth a definition that draws on that found in Article 49 (1) of Additional Protocol I: 'Attacks means acts of violence against the adversary, whether in offense or defense.' By this widely accepted definition, it is the use of violence against a target that distinguishes attacks from other military operations. Non-violent operations, such as psychological cyber operations or cyber espionage, do not qualify as attacks."

operation, this hack highlights the risks emanating from a lack of constraints on cyber actions. It likewise offers an opportunity for the Biden administration to identify a pathway toward clear, agreed-upon rules of engagement and propagation of norms in order to avoid miscalculation, chaos and even war.

It is against this backdrop that we explore the possibility of a U.S.-Russia cyber "rules of the road" agreement. We define rules of the road as actions within the cyber domain that the two parties agree not to commit for the purposes of preventing war, damage to systems, physical harm and/or deaths. In order to normalize relations and increase security writ large, we believe it would be in the long-term interests of both countries to eventually enter into a cyber rules-of-the-road agreement. Unfortunately, reaching such an agreement, in the current environment, is not immediately feasible. That said, the U.S. must begin now to consider the outline of an agreement and state definitively what it believes are acceptable and unacceptable activities in cyberspace, as building trust and goodwill and identifying opportunities to address key divergences in interests will likely take years. Below we delineate the contours of such an agreement, in hopes that this aids policymakers in devising short- and medium-term objectives toward the long-term and enduring goal of a more safe, secure and stable cyberspace. Even without a path to a formal agreement, we advocate for continued bilateral relations, including Track 1.5 or 2 dialogues, if only to keep a channel open during times of increased tensions, such as the ongoing SolarWinds fallout. One of the most important goals, in our view, would be a bilateral (or multilateral) ban on certain types of cyber operations against critical infrastructure, including all nuclear facilities and certain election infrastructure. This aim can be pursued outside the framework of a formal agreement and would be but one component of a comprehensive approach to defending such systems. The March 2021 U.N. consensus report on cybersecurity, backed by both Washington and Moscow, suggests the two sides are already committed to this goal[2]; however, agreement in the abstract leaves lots of real-world shoals to navigate. Moreover, as described below, we believe the list of targets that are off-limits would need to be narrowed down to make the rules effective.

2 See points (f) through (h) in the list of 11 voluntary, non-binding norms for responsible behavior of states in cyberspace recommended in the 2015 U.N. Group of Government Experts report (Appendix 1).

To inform this paper's arguments we have drawn upon a review of existing literature as well as interviews with 11 subject-matter experts, including current and former U.S. officials.[3] First, we address why it is in the long-term interests of both countries to establish such an agreement. Second, we discuss the roadblocks that must be overcome in order to negotiate a deal. Third, we examine the potential structure these rules of the road might take, as well as specific areas they might cover. Finally, we conclude by enumerating potential confidence-building measures that could be implemented by administration officials.

Why a US-Russia Cyber Agreement Is Needed but Currently Not Possible

We contend that it is in the national interests of both Russia and the U.S. to establish cyber rules of the road in the long term, for national and international security. Both countries are exposed to threats emanating from the cyber domain that can result in economic losses, political instability, erosion of public trust, extremist violence and other physical harm, as well as the destruction of military and civilian infrastructure. As the adversarial relationship between Moscow and Washington plays out in the cyber domain, where the distinction between defense and offense can be elusive, there is dangerous potential for miscalculation and unintended loss of control. Take, for example, NotPetya, the data-destroying 2017 cyberattack attributed by security researchers, the White House, the U.K. and other Western powers to Russian state hackers: Though aimed primarily at Ukraine, it raced around the globe affecting computers in more than 60 countries and causing an estimated $10 billion in damages, including huge losses for multinational private companies like FedEx, Maersk and Merck. The worm even struck Russian companies (including the crucial state-controlled oil behemoth Rosneft, though the damage there appears to have been "remarkably well-contained," according to NATO cyber-defense experts). Moreover, even when nations act with utmost care and due diligence in employing the cyber tools they create for their own use—as we believe tends to be the case in the U.S.—theft and leaks can still occur,

3 We have chosen not to name the current and former government officials among our interviewees so that they could speak candidly about sensitive subject matter.

sometimes with dire consequences: For instance, one of the main exploit tools allegedly used in NotPetya had reportedly been created by the United States—a claim that has not been confirmed—but wound up on a cyber-criminal black market a few months before NotPetya and WannaCry, a virulent ransomware also using the exploit, struck computers worldwide; since then, the tool has reportedly been used to paralyze infrastructure and extort entire U.S. cities.

The principal reason that establishing U.S.-Russia cyber rules of the road is currently not feasible is that the two countries' near-term cyber and related political goals appear diametrically opposed. Of top concern for the U.S. government, in our view, is stopping foreign interference and disinformation intended to undermine American democracy, protecting critical infrastructure, preventing or guarding against reckless malware and safeguarding confidential communications—with the associated threats emanating directly from Russia. One of Moscow's chief interests, on the other hand, according to a former CIA senior executive, is weaponizing cyber capabilities to sow discord and embarrass Western powers it views as undermining its sovereignty (principally the United States, especially in the wake of the unauthorized disclosure of classified NSA operations by Edward Snowden). Another Russian interest is maintaining control over domestic cyberspace to ensure political stability, according to an internationally recognized expert on cyber conflict.

In both cases, in our research-based assessment, Moscow sees a need and an opportunity to strengthen its geopolitical position and to counter what it perceives as malign Western influence or threats to its interests. Achieving these goals, as well as many others, is aided by aggressive cyber espionage, compromising networks, releasing sensitive information and disinformation operations aimed at the civilian population, business and infrastructure—in other words, the most vulnerable parts of the United States.[4] The limited nature of bilateral dialogues widens the chasm between the two countries: A U.S.-Russian working group on cyber issues was

4 In May 2020 the NSA warned that Russian military hackers had tried to steal emails through a program reportedly used by dozens of government officials and congressional candidates; in September, Microsoft issued a similar warning; in July, Wired reported, citing FBI documents, that a hacking group linked to Russia's military intelligence service had spent at least a year and a half targeting "a wide range of U.S.-based organizations, state and federal government agencies and educational institutions," plus, probably, entities in the energy sector. It is not clear whether any of the breaches in these reports overlap with the SolarWinds operation.

suspended shortly after its creation in 2013 in the wake of Moscow's armed intervention in Ukraine. Although some limited cooperation between the countries' officials seems to have continued, U.S. political will to engage the Russians on cyber issues is wanting. The SolarWinds hack, which compromised several U.S. government agencies' data and could have affected up to 18,000 customers of SolarWinds' network management system, does nothing to engender goodwill.

One might argue that during the Cold War Washington's and Moscow's interests were no less antipodal and their relations no less adversarial, yet they managed to sign some pivotal arms control agreements, including the bilateral 1972 Anti-Ballistic Missile Treaty (ABM), Strategic Arms Limitation Talks Agreement (1972 SALT I and 1979 SALT II) and 1987 Intermediate-Range Nuclear Forces Treaty (INF), as well as the multilateral 1963 Limited Test Ban Treaty (LTBT). One key distinction between those deals and potential rules of the road for the cyber domain lies in verification. Ensuring compliance with arms treaties involves rigorous on-site inspections, information exchanges and the ongoing monitoring of facilities. (NPT verification even relies on an independent U.N. body, the International Atomic Energy Agency, or IAEA.) These mechanisms have been critical to the continued success of arms control treaties. But "cyber verification is not the same as counting missiles," in the words of Robert Papp, a former director of the CIA's Center for Cyber Intelligence. In his opinion, "inspection and confidence-building visits to cyber and signals intelligence facilities are unlikely ever to be envisioned or even relevant," and the United States and Russia will have to think more creatively about verification under any cyber agreements.[5]

Nonetheless, we believe that attribution and verification of claims will be central obstacles to successful cyber agreements between adversaries. The challenge goes beyond the extreme unlikeliness that governments—particularly the U.S. and Russia—will allow inspections of their cyber-related facilities. In some instances when the U.S. has alleged cyber malfeasance by Russia in the past, a former Bush and Trump administration official told us, Moscow has asked for more copious evidence than U.S officials

5 Papp argued in 2019 that, as difficult as it may be, the United States should pursue a cyber treaty with Russia.

are willing to provide, loath to reveal classified information on methods or sources. Even when the U.S. has collected sufficient evidence for cyber-related indictments against Russian intelligence officers, Moscow has continued to deny involvement. This set of problems is exacerbated by a lack of consensus around the threshold of evidence required for definitive attribution of cyberattacks.

Finally, to go a step further, we argue that, given the current divergence of U.S. and Russian cyber-related priorities, any rules-of-the-road agreement right now would likely be counterproductive, if not detrimental, to U.S. interests. First of all, we believe it could hamstring U.S. cyber options, especially considering the likely lack of enforcement mechanisms and compliance verification, not to mention Russia's recent track record of noncompliance with other treaties. Second, particularly in light of past failed attempts at developing bilateral cyber guidelines, negotiations toward such a deal may simply serve as a maneuver that benefits Russia—whether as PR or as a means of advancing its vision of a "sovereign and controlled" internet. At the same time, these negotiations might waste U.S. resources and possibly undermine U.S. legitimacy, if the talks' failure is blamed on Washington.

Conditions Necessary for Negotiating a Successful Agreement

Greater alignment of interests is a necessary but not sufficient precondition for a successful rules-of-the-road agreement. Also necessary are conditions that, at their core, help build trust between the U.S. and Russia that negotiations are being undertaken in good faith and outcomes are reached through a fair process. We have identified five prerequisites in this regard, each of which is examined more closely below: codified procedural norms, the appropriate rank of participants on both sides, clear attribution standards, a mutual understanding of proportional retaliatory actions and "costly signaling." In our opinion all five are crucial: If even one of these conditions is not met––currently, not a single one is––the agreement may not succeed.

First, we believe that costly signals—or high-cost actions undertaken by one party to provide assurance to the other—are necessary to overcome decades of mistrust and to convey sincere intentions and a credible commitment to reaching a mutually beneficial agreement.[6] As many of our interviewees indicated, there is deep-seated "Russia fatigue … inside the Beltway," in the words of a congressional staff member, with U.S. officials and experts exasperated by what they see as Russia's adversarial intentions, betrayals of trust and justifications designed to avoid genuine cooperation. Conversely, according to an expert on Russian negotiations, Moscow believes that the United States is not interested in generating trust based on continued rejections of calls and letters. Costly signals, combined with a closer alignment of interests, may be the only mechanism that can overcome this fatigue and catalyze negotiation.

The U.S. and Russia could choose from a range of costly signals, but we believe that actions addressing the key concerns of the other country—for example, stopping Russian-executed disinformation operations—would likely be most effective. In practical terms, Moscow could shut down operational "troll farms," which have been central to its recent disinformation efforts; crucially in our view, the U.S. can measure and verify such actions through online content monitoring. Of course, the U.S. and its allies would need to be convinced that this action was not simply masking other attempts by Russia to undermine the U.S. public's trust, but it could convey goodwill. The United States' reticence to engage with Russia reflects deep suspicion after several high-profile cyber operations and wariness of being taken advantage of after several attempts to negotiate in multilateral fora. Costly signals acceptable to Moscow would have to be investigated further, though the above-mentioned expert in negotiating with Russians suggested that cheap signals may be a better starting point.

Second, we feel that codified procedures for negotiations will help decrease unintended escalation of tensions and facilitate trust. More specifically, prior to the start of talks, we believe that both parties should agree upon a clearly defined timeline and set list of topics to address in the discussions.

6 Fearon, James D., "Signaling Versus the Balance of Power and Interests: An Empirical Test of a Crisis Bargaining Model," *The Journal of Conflict Resolution* 38 (2), 1994, pp. 236-269; Fearon, J. D., "Signaling Foreign Policy Interests: Tying Hands versus Sinking Costs," *The Journal of Conflict Resolution*, 41 (1), 1997, pp. 68-90; Kydd, A. H., "Trust and Mistrust in International Relations," Princeton University Press, 2005.

The U.S. and Russia must furthermore decide how the cyber negotiations fit within the broader bilateral relationship and geopolitical context. For example, are the talks part of discussions on arms control or will they be kept separate? A transparent, synchronized understanding of the negotiation procedure, in our view, can help keep these talks from poisoning other contentious political discussions and can decrease the potential exploitation of procedural gray areas for the benefit of a single party, increasing trust in the process. A similar understanding of the elements of one another's cyber mission priorities, intents, capabilities and organization will also help to identify key players and command structure.

Third, the U.S. and Russia must be represented by parties of equal "rank," with sufficient authority and support from their respective governments to ensure that negotiated commitments are realized. For U.S.-Russian negotiations, "rank mismatch"—which could be obvious or inconspicuous—may pose a genuine obstacle if the officials from one country have a significantly different level of authority than those from the other country. For example, while representatives of the U.S. State Department often speak for their government's executive branch, some of our interviewees have indicated that Russian diplomats sometimes carry less authority or "lack the ear" of the Kremlin. If this is indeed the case, the Russian delegation must include individuals who hold sway with Moscow's chief decision maker, President Vladimir Putin, in the opinion of one former official from the Bush and Trump administrations. The U.S. delegates should likewise hold sway with key stakeholders in the legislative and executive branches. Given the United States' political discord in recent years, many nations grew to believe there is no single voice accurately representing the U.S. position, according to two of our interviewees. The change in administration may alter this perception since President Joe Biden is seen as a return to more orthodox diplomatic procedures, but Washington will have an uphill battle in assuaging concerns that representatives in such talks will not be undermined by other domestic actors in the present or future. It is equally important that the parties represent the appropriate organizations to achieve stated objectives during official discussions. Negotiations will require expertise not only in diplomacy and the law but also in cyber operations, threat and attribution and other operational and technical elements. The bottom line: Each side must have faith that its negotiating counterparts

truly represent their nation and its position on the issues and that their statements and concessions are not meaningless.

Fourth, we believe that clear attribution standards for identifying the actors behind particular cyber activity are necessary to enforce a rules-of-the-road agreement and verify compliance. Developing such standards has been difficult even for close allies, much less adversaries. The above-mentioned Tallinn Manual 2.0—a 2017 attempt to apply existing international law to cyber operations, undertaken by NATO's Cooperative Cyber Defense Center and written by a group of 19 experts on international law—does not provide clear guidelines for attribution. Instead, it explains what attribution is not by noting that using governmental cyber infrastructure or malware that "is designed to 'report back'" to governmental infrastructure is "usually insufficient evidence for attributing the operation to that state."[7] In the absence of clear standards of attribution, it is easy for an accused party to dispute evidence, deny responsibility and/or simply keep mum.

Agreement between the negotiating parties over what exactly constitutes a "smoking gun" would obviously make it far more difficult for the accused party to dispute the evidence. One possible solution, according to a former NSA cyber expert, would be to involve experts from the private sector and from academia to develop and codify attribution guidelines for third-party and private sector entities. Another solution may be to create an international standards body for attribution that would set the minimum thresholds and technical standards for attribution for public and private sector use; if parties were to agree on such thresholds and standards, the process of attribution would become transparent and indisputable (if not conclusive). This would bolster both governments' ability to attribute cyber incidents using open-source information without exposing or jeopardizing their own sources or methods.

Fifth, we believe that a successful agreement requires a mutual understanding of proportionality between the U.S. and Russia. In other words, both parties must agree on the appropriateness of certain retaliatory actions in cyberspace. An example of a hypothetical disconnect is that the

7 See "Chapter 4: Law of International Responsibility," p. 91 in print edition (Cambridge University Press, 2017).

United States, as the finance capital of the world, might perceive a highly costly ransomware campaign against a bank's payment infrastructure as a destructive cyberattack, while Russia perceives it as a nuisance. To prevent miscommunication or mismatched retaliation, both sides must reach a common understanding of one another's positions regarding perceptions of certain cyber actions, according to the internationally renowned cyber policy expert cited above. We believe that this objective is best accomplished via communication of red lines, which we view as both part of norm-setting and a confidence-building measure through dialogues, described in more detail below. In addition to understanding these red lines, the former senior CIA official told us, both countries must have a clear understanding of how each side will retaliate if a given action is taken or a certain red line is crossed; this shared understanding will help prevent miscommunication and unintended escalation.

Structure of a US-Russia Cyber Agreement

As noted above, pursuing an agreement now would be premature and could unduly restrict U.S. options in the cyber realm, and even inflict reputational damage if public perceptions of the talks are manipulated to that effect. That said, the potential long-term benefits to the U.S. government of a genuine, effective cyber agreement with Russia include: de-escalation of tensions; protection of U.S. national interests (increasing security, protecting citizens and strengthening public trust in elections among them); and the establishment of norms and rules within cyberspace that can apply on an international scale. An optimal deal would obviously result in a symbiosis whereby both countries feel a decreased level of risk vis-à-vis one another. In aspiring to such an agreement, below we consider some basic questions about what form it might take.

1. Should the rules be formal or informal?

While getting bilateral cyber rules of the road through the U.S. Congress would be a significant hurdle, we strongly believe that any substantive agreement should take the form of a formal treaty requiring Senate

approval for ratification. Given the polarization within U.S. politics when it comes to Russia, any unilateral executive branch action could easily fall victim to political infighting, regardless of which party is in power, according to one former Trump administration official. We also acknowledge the potential for members of Congress to use a debate for political theater, which is why we recommend bipartisan introduction and support within a congressional committee like the Senate Foreign Relations Committee, Senate Armed Services Committee or Senate Committee on Homeland Security to ensure a thoughtful debate. Several recent bipartisan efforts on cybersecurity suggest potential appetite for taking up this issue. The legislative branch will likely want input on enforcement mechanisms, such as potential snapback sanctions for violations. Thus, according to the same former Trump presidential administration official, the most promising path to a viable agreement is to reach consensus, involving the legislative branch in addition to the executive branch.

2. Should the treaty be bilateral or multilateral?

Although a multilateral treaty is appealing as a means of decreasing cyber threats, we believe a rules-of-the-road agreement between the U.S. and Russia should be bilateral. Multilateral treaties run the risk of preventing the "customization" necessary to fit the specific context of the U.S.-Russian cyber relationship. If more countries were involved in these discussions, conflicting interests could result in a weak agreement. Furthermore, we feel that a bilateral agreement will allow the U.S. to have greater control over the narrative surrounding negotiations on the international stage. Russia has used multilateral institutions, including the U.N. Group of Governmental Experts on cybersecurity and Open-Ended Working Group on cybersecurity to advance its own conceptualization of cyber norms, sometimes undermining Western influence.[8] Although a bilateral agreement with Russia would also likely necessitate a separate agreement with China, we consider it to be the most viable mechanism to engage

8 For examples see: Stronski, Paul and Richard Sokolsky, "Multipolarity in Practice: Understanding Russia's Engagement With Regional Institutions," Carnegie Endowment for International Peace, Jan. 8, 2020; Moreland, Will, "The Purpose of Multilateralism," Brookings Institution, Sept. 23, 2019; Achten, Nele, "New U.N. Debate on Cybersecurity in the Context of International Security," *Lawfare*, Sept. 30, 2019; Sherman, Justin and Mark Raymond, "The U.N. Passed a Russia-Backed Cybercrime Resolution. That's Not Good News for Internet Freedom," *The Washington Post*, Dec. 4, 2019.

with Russia over cyber rules of the road. We also believe that a bilateral agreement with Russia could have a positive ripple effect, as other nations grappling with similar issues will look to two of the most cyber-capable nations in the world to codify and abide by these norms.

3. Key definitions within the agreement

In order to successfully codify cyber rules of the road, a crucial first step, in our opinion, is to ensure that the U.S. and Russia agree on the definitions of key terms in the cyber realm—many of which currently fall in gray areas or leave significant room for subjective interpretation. In this section we enumerate the terms we believe can and should be defined. Recognizing the immense work already undertaken in this area, we take as our basis the 2014 "Critical Terminology Foundations 2" report jointly written by the U.S.-based EastWest Institute[9] (EWI) and Russia's Information Security Institute (ISI), which offers 40 shared U.S.-Russian definitions for cyber-related terms. Given the rapid pace of developments within the cyber realm, as well as changes in U.S.-Russian cyber relations, many of the definitions in the report are outdated. Understanding how quickly terminology in the domain evolves (e.g., the term "information operation" has changed over the past decade[10]), we believe that attempts to fully agree on all relevant definitions are futile. However, some modicum of agreement must exist to ensure that any cyber deal is understood the same way by both sides. Below, we first list which definitions from the EWI-ISI report we consider acceptable for use in present-day rules of the road; next, we critique certain definitions that we believe to be flawed or outdated.

The EWI-ISI report splits its definitions into three separate categories: "The Theater" of cyber warfare, "The Modes of Aggravation" and "The Art," which includes general terms related to the cyber domain. Overall, we broadly agree with the 11 definitions under the "Theater" category, as these terms are relatively neutral from a political or military perspective.

9 EastWest's programs on cyber issues were transferred early in 2021 to Observer Research Foundation America.

10 For varying definitions of the term "information operation" see: Brunetti-Lihach, "Information Warfare Past, Present, and Future"; Paul, "Is it Time to Abandon the Term Information Operations?"; Cicalese, "Redefining Information Operations."

For example, possible definitions of "cyber forces" (part of "Theater") are far less divisive than those of "information operation" (in "Modes of Aggravation"). We will note, however, that even some of the "Theater" terms would need to be clarified for any cyber rules of the road—for example, are privately held banks with assets under $500 million considered "critical cyber infrastructure" or not?

On the other hand, we believe that many of the definitions under the "Modes of Aggravation" and "Art" categories are far from adequate. Rather than try to cover all of these, we have opted to critique four specific terms in order to elucidate our overarching viewpoint on the nature of the inadequacies: cyber espionage, cyber conflict, cybercrime and cyber operation.

- Cyber espionage is defined as "a cyber operation to obtain unauthorized access to sensitive information through covert means." As stated in the executive summary, the SolarWinds breach was a major cyber espionage operation, but it and other reconnaissance operations that were intended to map U.S. critical infrastructure have gone beyond traditional espionage. Indeed, the term cyber espionage does not accurately describe the full impact—or, in our view, the intent—of the operations because they are capable of "holding targets at risk." This is a different category of operations, whose key mission, in the words of Michael Sulmeyer and Ben Buchanan, is to "seek to develop offensive capabilities against possible future targets." In other words, cyber espionage can provide perpetrators the access and ability to execute cyberattacks on the targets of their reconnaissance. To reflect this category of threat, a new term should be introduced into the common lexicon.
- Cyber conflict is defined as "a tense situation between and/or among nation-states and/or organized groups where unwelcome cyberattacks result in retaliation." One clear problem with this definition is the use of the terms "nation-states and/or organized groups." Russia, for example, has reportedly relied on individual hackers who may not fit the criteria for "organized group." Moreover, cyberattacks do not always result in retaliation. Attribution to nation-states, as noted above, is also difficult. The Tallinn Manual 2.0, for instance, says that actions conducted by

non-state actors under the "effective control" of a state are attributable to a state but does not clearly define "effective control."

- Cybercrime is defined as "the use of cyberspace for criminal purposes as defined by national or international law." This definition is too broad to be useful. First and foremost, Russia and the U.S. have vastly different national laws and legal traditions and do not always agree even on international law. Russia has not signed on to the 2001 Convention on Cybercrime, which attempted to "harmonize cybercrime legislations across countries" and has been ratified by the U.S. (albeit with reservations); moreover, Russia has been lobbying for years in international fora to create an alternative cybercrime convention. In short, any language on cybercrime would have to be far more specific to have any utility.
- Cyber operation is defined as "organized activities in cyberspace to gather, prepare, disseminate, restrict or process information to achieve a goal." Our critique of this definition involves its focus solely on "information": Does the theft of money or the destruction of hardware and physical infrastructure not constitute a cyber operation if carried out using cyber means?

The bottom line is that many of the EWI-ISI definitions are too vague to work in a formal U.S.-Russian cyber agreement. Furthermore, fast-paced developments can quickly render definitions outdated, even when they seemed sufficiently specific at first. For example, would COVID-19 vaccine research, which Russian actors have been accused of hacking, have represented "critical cyber infrastructure" at the start of 2020? Does it now? While clarity surrounding key cyber terminology is crucial for successful rules of the road, the only universe in which suitable definitions might be developed is one in which both the U.S. and Russia carefully observe one another's behavior and continuously engage in bilateral dialogue about what they consider acceptable and unacceptable behavior. In other words, the definitions should be easy to update and amended as new developments arise. Only by allowing such evolution and flexibility is a sustainable agreement possible.

4 . Which sectors of the cyber domain should these rules cover?

This section assesses potential areas that might be covered by U.S.-Russian cyber rules of the road.

Espionage

There is no scenario in which the U.S. and Russia would agree to bar cyber espionage wholesale. First, as noted in Rule 32 of the Tallinn Manual 2.0, "peacetime cyber espionage by states does not per se violate international law."[11] In other words, cyber espionage would only be barred if it violated a bilateral or international agreement or some other law.[12] As the former senior CIA official pointed out, both countries continue to see a benefit in cyber espionage and would likely not want to limit their ability to use it. However, as more information materializes from the SolarWinds operation—such as whether the perpetrators damaged informational or operational systems, put lives in jeopardy, caused death(s) either directly or indirectly or emplaced malware designed to destroy or damage systems—experts and policymakers alike will debate the nuances of espionage and associated activities in cyberspace and their impact in the physical domain. Regardless, we must underscore that this operation targeted government networks as well as civilian infrastructure and businesses.

We also want to draw attention to the fact that the line between "espionage" and "cyberattack" can be very thin. How can one prove that a network or database was simply snooped on by a counterparty? Can one be sure that a backdoor or malicious code was not inserted surreptitiously? We must be clear about the characteristics that distinguish certain operations as merely espionage versus something more insidious, such as preparation for attack or holding targets at risk; in fact, it may be useful to describe a spectrum of malicious activity, tipped one way or the other only by a few keystrokes. One set of questions to consider is whether a certain activity or action is offensive (i.e., aggressive and perpetrated against another party)

11 See "Chapter 2: Due Diligence," p. 35, in print edition referenced above.

12 It must be noted that espionage, while not violating international law per se, is a crime in many nations. In the U.S., for example, it is addressed by the Espionage Act of 1917, the Economic Espionage Act of 1996, Chapter 37 of the U.S. Code and other laws and regulations.

and intended to harm, influence, achieve an objective or affect an outcome. And another set of questions should address whether that operation targets, either purposefully or not, civilians and civilian infrastructure and businesses, and violates a nation's sovereignty in doing so. Again, in examining the finer points and impact of the SolarWinds operation, we have an opportunity to help clarify our views on what is and is not appropriate in cyberspace and declare our intent in light of that clarification.

Attacks on Critical Infrastructure and Reckless Activities in Cyberspace

An agreement to bar certain attacks on critical infrastructure would be the most important inclusion in bilateral cyber rules of the road, in our opinion, and some version of it could be pursued within a less formal framework as well. The U.S. has identified 16 critical infrastructure sectors deemed vital to U.S. security, public health/safety and national economic security,[13] though the list is quite broad. In 2017 DHS designated election infrastructure as critical as well. If the U.S. and Russia could roughly agree on these designations, and given that both countries would benefit from a decrease in cyber intrusions targeting these systems, the two should consider pursuing rules of the road concerning attacks on or intrusions into these areas. Such prohibitions, as noted before, may require whittling down the list of banned targets and would certainly apply to nation-states; ideally, they would cover non-state actors operating at the behest of a state or with its tacit support, as well, but this is a thornier question that is likely to require lengthy negotiations. It is also worth noting that in the United States critical infrastructure is mostly civilian-owned and -operated, a point brought up in the Elbe Group dialogue on cyber in October 2019. An article published in 2020 describes Russian critical infrastructure as run by the state and by private companies with the goal of a "unified state system." This difference between the two countries highlights how differently they may interpret those portions of the Law of Armed Conflict that concern distinguishing between combatants and civilians as well as proportionate

13 The 16 sectors are: chemical; communications; commercial facilities; 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 wastes; transportation; and water and wastewater systems.

damage to civilian lives and infrastructure. Of particular concern, we believe, would be cyber activities that impact election infrastructure and commercial and military nuclear systems (including weapons systems), as well as attacks on critical infrastructure resulting in material damage, loss of life, and other physical harm.

a. Election infrastructure and processes

Many U.S. policymakers consider the protection of domestic election infrastructure to be of utmost importance, with one former senior military official whom we interviewed classifying it among the key national interests existing today. Below, we critique a few existing proposals that a bilateral agreement could potentially draw upon and suggest narrower rules that may be most acceptable to both Washington and Moscow.

Both the Tallinn Manual 2.0 and the Paris Call for Trust and Security in Cyberspace offer bans on election meddling, but these are likely too broad for inclusion in U.S.-Russia rules of the road. The former bars states from intervening, "including by cyber means, in the internal or external affairs of another state,"[14] while the latter proposes an expansive norm arguably most in line with U.S. interests: "Defend electoral processes: Strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities." Moscow has long viewed U.S. support for certain NGOs and other political actors operating in Russia as interference in its affairs; the Paris wording, moreover, would entail a hard-to-achieve level of verification and enforcement.

However, rules that narrowly focus on technical infrastructure—for example, forbidding illicit changes to ballots or hacks of election software and hardware—may be the most palatable for both sides. One such norm was proposed by the Global Commission on the Stability of Cyberspace (GCSC): "State and non-state actors must not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites." The Tallinn Manual 2.0 says that activities that "alter electronic ballots and thereby manipulate an election"

14 See "Chapter 13: Prohibition of Intervention," p. 312, in print edition referenced above.

would violate international law.[15] The lack of evidence that a foreign actor attempted to alter technical aspects of the 2020 U.S. presidential elections may indicate growing alignment on such a rule.

b. Civilian and military nuclear systems

We believe the U.S. and Russia should consider barring all cyber activities on each other's nuclear systems, including both civilian nuclear power facilities and military nuclear weapon systems. The potential for nuclear catastrophe or unintended miscalculation that leads to nuclear war poses too great a risk to allow even cyber espionage on certain systems, in our view. In the SolarWinds hack, a terrifying precedent was set via the breach of the DOE as well as the National Nuclear Security Administration. We strongly believe that a reciprocal continuation of this trend will end in disaster.

Going forward, the U.S. and Russia might leverage work undertaken by the Nuclear Threat Initiative's Cyber-Nuclear Weapons Study Group to establish norms to not attack nuclear communication, command and control (C3) systems and other nuclear weapons systems. As noted in the group's 2018 report, the U.S. and Russia would also benefit from communicating their red lines pertaining to cyber activities on nuclear facilities, indicating which activities would be considered an act of war or warrant serious retaliatory actions.

c. Attacks, whether targeted or indiscriminate, on civilian critical infrastructure resulting in material damage, loss of life, or other physical harm.

Finally, we believe the U.S. and Russia should pursue norms that seek to prevent targeted or indiscriminate intrusions and attacks leading to material damage, disruption/destruction of critical processes or services

15 Ibid., p. 313.

and loss of life or other physical harm, particularly among civilians.[16] An example of such an attack could be shutting off a power grid, disrupting gas pipelines, tampering with the water supply and impacting hospitals and killing or otherwise adversely affecting patients. In a similar vein, state actors should be held responsible for attacks like NotPetya and WannaCry as cyber-weapons operators and, much like with conventional weapons and conflict, should be compelled by international law to discriminate between civilian and military targets. (The Paris Call's first principle is to "protect individuals and infrastructure," calling on parties to "prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure." Although theoretically desirable, the breadth of this recommendation again makes it very difficult to implement. For example, the U.S. and Russia would need to agree on the meaning of "significant, indiscriminate or systemic harm," as well as guidelines for demonstrating a state did all it could to "prevent and recover from" or "protect" individuals from an indiscriminate, potentially unintentional, attack.)

We must underscore the historical precedents for Russian cyber espionage, mapping, intrusion and disruption of critical infrastructure, particularly in Ukraine with Russia's alleged success in disabling electrical utility grids for hours first in 2015 and then in 2016. Both events were preceded by espionage efforts and the mapping of industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems. Each event demonstrated significant understanding of ICS/SCADA systems and increasingly sophisticated malware. Similar mapping of U.S. electrical, water and nuclear ICS/SCADA systems by Russian actors has been ongoing at least since March 2016, two years before the U.S. released its first report

16 It is helpful to refer to LOAC for context. Four principles undergird LOAC and are thoroughly integrated into U.S. military practice. First, armed groups must distinguish between combatants and non-combatants (or civilians). The principle of distinction dictates that armed groups must target combatants and military objects, avoiding the intentional targeting of civilians and civilian objects. Second, any armed attack against military targets must be proportional. Specifically, incidental or collateral damage must be minimized to the greatest extent possible and must be proportionate to the military advantage obtained through the operation. In other words, excessive use of force is impermissible. Third, the attack must be militarily necessary to weaken the opponent and, fourth, the weapons and tactics used are limited to those that do not cause indiscriminate or unnecessary suffering or injury. In order to ensure all four principles are met, states are supposed to undergo precautionary measures and do "everything feasible" to ensure the operation will proportionally target military objectives, while minimizing unintended loss of life or damage to civilian objects. The International Criminal Tribunal for the Former Yugoslavia explained that the standard to determine whether these principles, particularly proportionality, were followed would be a "reasonable well-informed person in the circumstances of the actual perpetrator, making reasonable use of the information to him or her." An analysis of the application of LOAC to an incident should therefore not be overly technical in nature.

publicly attributing such activity to Russia. Economic sanctions against Russia were levied in 2018 in response to this cyber activity. While there was no apparent physical impact, the activity still presents danger to our security.

Should the US and Russia Pursue Confidence-Building Measures and, if So, Which Ones?

Although we believe that a formal cyber rules-of-the-road agreement would be the ideal mechanism for establishing norms, de-escalating U.S.-Russia tensions and furthering U.S. national interests as they relate to the cyber domain, there is room in the short and medium term for the adoption of confidence-building measures by both countries. Such measures would involve actions that can be taken before, during and after the establishment of agreements and can catalyze more substantive diplomatic engagement while also preventing unwanted escalation or misunderstanding. U.S.-Russia confidence-building measures must invariably be evaluated and developed on a case-by-case basis. The most useful of them, in our view, fall into two broad categories: dialogues and joint initiatives.

Dialogues

Dialogues refer to any communication between the two nations that relates to cyber action. The principal benefits of such dialogue, based on our interviews with military and CIA officials, include the communication of red lines, warnings of potential retaliation, explanations of intent and clarification of definitions and terminology.[17]

Dialogues could take place as Track 1, 1.5 or 2, with the latter two being the most feasible at this point. The tactical benefits of this form of discussion are two-fold. First, in the words of the internationally recognized expert on cyber conflict, they are a low-cost way to "keep the conversation going."

17 While we think that terminology/definitions are a crucial aspect of any future rules-of-the-road agreement, we also believe that discussing this subject outside the context of such an agreement is highly useful.

For example, "formally informal" discussions allow the sides to gauge who genuinely holds sway within governments, to build personal relationships and to exchange information and concerns. Such dialogues also let the U.S. and Russia share information on an as-needed basis about particular threats faced by each country. For example, the U.S. could give Russia advance warning of North Korean malware that is making its way across the internet, or vice versa. Such threat sharing can be an effective way to build goodwill between the nations, according to the former NSA cyber expert we interviewed. While Track 1 dialogues can more easily precipitate behavioral change than lower-level discussions, we believe such dialogues will not be fruitful without credible costly signaling to reassure officials that their time and resources are not being wasted.

There are a number of Track 2 dialogues between the U.S. and Russia, primarily in the think tank and academia domains, that are important for information exchange, especially in the absence of formal discussions. The Center for Strategic and International Studies held such a dialogue on crisis stability between 2017 and 2018, while the National Academy of Sciences currently engages experts from the Russian Academy of Sciences in an ongoing dialogue on a variety of security issues, including cyber. The EastWest Institute was active within this space, having launched a military-to-military Track 2 dialogue in fall 2020, which will be continued by the Stimson Center, and released a report with the Russian International Affairs Council on cooperation between the two nations on cybersecurity, as well as a report with the Russian Institute of International Information Security Issues at Moscow State University. And finally, the Belfer Center for Science and International Affairs hosts the Elbe Group Track 2 dialogue with former senior military and intelligence officials from the U.S. and Russia meeting twice per year to discuss strategic security issues. In 2019, the group met in Stockholm, Sweden, principally to discuss bilateral cybersecurity, with one of this paper's authors, Belfer Cyber Project executive director Lauren Zabierek, taking part and raising concerns about malware and critical infrastructure; ultimately, the Elbe Group members publicly expressed their "opposition to creation or employment of weapons to attack critical infrastructure." These meetings should continue and specifically focus on cybersecurity in order to keep the dialogue open, exchange information and find areas of common interest.

Joint Initiatives

Joint initiatives, in contrast to dialogues, are characterized by communication and actions toward specific deliverables. Such initiatives build on areas of overlapping interests, while also helping both countries advance their own national security goals; they can act as a foundation for more productive interaction in the future. It must be noted that such measures should be undertaken further in the process of discussions to lay the groundwork for trust and political will toward an end-state agreement. Engaging in such measures prematurely would, in our view, jeopardize the process because either side may feel its goodwill is being taken advantage of or officials taking part in the activities may suffer adverse effects from the extreme politicization of the bilateral relationship.

One potential example might include collaboration on combatting international financial cybercrime, especially the sort that poses risks to life, health and/or critical infrastructure. One approach, for instance, would involve the formation of a joint committee made up of cybercrime officials from both countries. Theoretically, the U.S. and Russia share an interest in decreasing the threat posed by materially driven cybercrime, particularly by actors targeting both countries and inflicting significant economic damage. Russia's Sberbank estimated in 2017 that the country's annual losses to cybercrime total between about $10 billion and $11 billion. The U.S. loses an estimated $11 billion annually to intellectual property theft alone, according to McAfee, a commercial cybersecurity firm; and ransomware may have cost the U.S. more than $7.5 billion just last year, according to another such firm, Emsisoft.[18]

However, the two countries' previous failures to agree on means of preventing or interdicting cybercrime, compounded by some of Russia's recent actions, suggest that the realistic scope of cooperation would be extremely limited. First, it is not clear whether Russia has a better ability than the U.S. to identify cybercriminals; moreover, in at least four recent cases Moscow has tried to prevent rather than abet extradition to the U.S. of Russian nationals accused of cybercrimes there. Second, some branches of the

18 Perhaps some mutually acceptable approaches could be found in the 2018 Paris Call for Trust and Security in Cyberspace, which includes language on preventing cyber-enabled theft of intellectual property.

Russian authorities are believed to have co-opted criminal hackers, using them to gather information or execute cyber activities at the state's behest; in 2017, the U.S. Justice Department announced indictments against two Russian FSB officers and two cybercriminals with whom they allegedly collaborated. With this track record, it may be hard to convince the U.S. government that Russia will genuinely work to decrease cybercrime.

While we believe that the above-described confidence-building measures can act as helpful building blocks on the road toward a substantive agreement, it is important not to overstate their feasibility. Positive outcomes are much easier theorized than practiced, and such measures take time and diligence that may be hard to come by. Nonetheless, we believe keeping the lines of communication open, even on an informal level, is necessary in this environment.

Conclusion: Long Road Ahead

Realistically, the U.S. and Russia will not agree on binding cyber norms in the near term, especially in light of the SolarWinds operation. Oppositional and sometimes antagonistic interests, deep-seated mistrust and a lack of mutually accepted attribution and verification mechanisms pose nearly insurmountable obstacles for the foreseeable future. Yet cyber represents a fundamentally new domain for conflict, one in which the rules have not been established. Like the introduction of aerial warfare at the turn of the 20th century, cyberattacks represent a new mode for lethal force, the destruction of critical infrastructure and espionage. But unlike air power, cyberspace can also be weaponized for financial crime, informational operations that are much speedier and more far-reaching than dropping leaflets from planes and widescale damage to critical infrastructure without the physical deployment of personnel and assets. As such, we believe the SolarWinds breach presents the Biden-Harris administration with an important opportunity to declare norms and rules within cyberspace that can apply on an international scale.

The cyber domain is rife with complexity, intangibility and "gray" areas. This makes it exceedingly easy for politicians to simply give up and hope for the absence of mass catastrophe. This is in complete disregard to a country's responsibility to its citizens. In this paper we attempt to provide concreteness to the notion of a future U.S.-Russian cyber agreement because we strongly believe that governments must be proactive rather than reflexive in this domain. Our aim is to provide a long-term pathway toward a potential agreement that helps avoid miscalculation, chaos and even war.

While it may be quixotic, enumeration is the first step to action. We propose five necessary conditions that the U.S. and Russia must meet to engage in productive negotiations: give costly signals, codify negotiation procedures, ensure that the right stakeholders are involved, develop attribution standards and reach a shared understanding of proportional retaliation. To be most successful, we believe this agreement should be formal, bilateral and focused on attacks and intrusions into critical infrastructure, electoral processes and nuclear command, control and

administration. Confidence-building mechanisms, in the form of dialogues and, if the conditions allow, joint initiatives, are necessary in the near term both as a stop-gap measure in the absence of a full agreement and as a means by which the United States and Russia can catalyze the fulfillment of the five conditions necessary to enter negotiations that offer better chances for success.

Prospects for US-Russia Cyber Rules of the Road: A Russian Perspective

By Pavel Sharikov

Over the past 30 years, the development of cyberspace has been mostly chaotic and minimally regulated. On the world stage, information and communication technologies, or ICTs, have emerged as many things at once: valuable public and private domestic resources; effective tools of international power, sometimes used aggressively; and a global domain. This liminality of ICTs and the internet itself—neither fully domestic nor fully global, fully public nor fully private, fully virtual nor fully physical—has led to legal and political tensions, with the cyber sphere becoming a new field of contention and every nation building its cyber capabilities and rules of governance in accordance with its own political traditions, realities and interests.

As ICTs have become essential in a wide array of critical sectors—from health care and banking networks to power plants and weapons systems—the lack of uniform rules of conduct for nation-states in cyberspace has become increasingly problematic, not least of all because cyber-enabled contention can have an unpredictable domino effect on civilian populations. In recent years, there have been attempts to come up with international cyber rules of the road. Yet several of the internet's defining features have made it difficult to constrain by international norms like the ones for sea, land, air and even space—in particular, its highly decentralized nature, lack of physical borders, relatively low cost and reliance on the private sector. Any effective system of international cyber rules of the road would need to strike a balance between competing national and international interests, as well as military and civilian concerns and government and private sectors. This is tough terrain to negotiate in the best of times; attempting to do so amid adversarial relations such as those currently plaguing Russia and the U.S. is outright daunting.

Nonetheless, while the path to full-fledged international cyber norms will be long, and a binding Russian-U.S. cyber treaty is out of the question at least for now, it is imperative that Russia and the United States—two countries with starkly opposing views on information/cyber policies—reinvigorate their dialogue on bilateral cyber rules of the road. Without candid communication and a bare minimum of clear rules, the risks of unintended escalation grow higher—in part, because it is difficult to gauge what sort of cyber operation could trigger an escalatory cycle of responses and counter-responses. Within the past few years, the U.S. has accused hackers believed to be working for the Russian government of infiltrating U.S. power grids and reportedly retaliated in kind. More recently, U.S. allegations of Russian state involvement in the SolarWinds hack, denied by Moscow but already punished by Washington, have highlighted the dangers of a blurred line between cyber espionage and cyberattacks—adding further uncertainty about possible responses. Each side has accused the other of interfering in its domestic affairs, for example by meddling in elections and stoking citizens' protests, and of behaving irresponsibly in cyberspace. The two countries must urgently find ways to chip away at the sense of total mistrust now characterizing relations between them. Here, in my view, are some first-order areas on which to focus:

1. The two governments should strive to **distinguish between cyber cooperation and competition**—between areas where they can work together against third parties and those where they are negotiating about the rules for working against each other. I envision this distinction as one between a diplomatic track and a military track. The two approaches would be complementary and partly overlapping, not mutually exclusive.

2. Find the political will for **greater transparency and respectfulness, drawing on decades of arms-control experience**. Russian diplomats have long insisted that Russia does not use cyber tools offensively and that cyber means should not be used in the military realm. Moscow must acknowledge that it cannot convince Washington, or indeed some of its own allies, to accept this position and should be willing to discuss military aspects of cyberspace. A refusal to do so effectively dumps all cyber issues—existential and not—in a single heap, hampering progress on high-stakes mutual

threats because they are entangled with, and excessively politicized by, issues that are lower-stakes but more controversial. Washington, for its part, must be willing to tone down its harsh public language against Moscow and be more judicious both in analyzing cyber operations believed to be emanating from Russia and in meting out punishment for those operations. Like during the Cold War efforts on arms control, these steps should be taken for the sake of mitigating potentially catastrophic threats. And just as Moscow and Washington were "doomed to cooperate" in the nuclear domain, so, too, are they fated to interact in global cyberspace, where, I believe, candid, constant dialogue will prove much more fruitful than bans and prohibitions.

3. The key goal is to **communicate red lines** and **establish thresholds for military retaliation** and other kinetic consequences. While most nations, including both Russia and the U.S., will want to retain the right to conduct espionage, doing so in cyberspace poses special risks, as computer code implanted for spying can be hard to distinguish from code intended to do damage.

4. Previous obstacles notwithstanding, Moscow and Washington should try to **resume confidence-building measures,** including, possibly, cooperation against materially driven cybercrime.

5. Initiate a bilateral effort to **clarify cyber-related definitions**, based on work not only by nongovernment experts but by U.S. and Russian officials as well.

6. The two sides should also explore ways to **involve more stakeholders** in bilateral talks on cyber norms, first and foremost from the private ICT sector. This may help the two sides develop common protocols for attribution of cyber operations without the fear of divulging sensitive state-controlled information.

As this paper seeks to demonstrate, Russia and the United States see the scope of government functions in cybersecurity very differently. In order to reach more realistic agreements on each state's responsibilities in this field, the two should focus on areas of overlap in government functions and ask one another only for that which each respective executive branch

can deliver. This premise undergirds the idea of a separate military track for cyber talks, since both countries' militaries are presumably under their respective governments' full control. (Both sides' diplomats also presumably answer to their respective capitals, and the civilian track of cyber relations is equally important, but it is more likely to be complicated by politics and the operations of cyber actors that neither state controls.)

Fortunately, there has not yet been a "cyber Pearl Harbor," but it is clear that as long as cyberspace remains so full of ambiguity, without formal, mutually accepted regulations—or, at least, clear red lines—it will be a source of potential unwanted escalation. Two U.S. experts have noted that of 272 major documented cyber operations involving nation-states in 2000-2016 most have not led to escalatory responses; they argue, however, that recently adopted U.S. policies emphasizing offensive cyber operations "increase the risk of escalation while doing nothing to make cyber operations more effective." Establishing cyber rules of the road would make Russia's and America's behavior more predictable, in my view, which would in turn improve global security. After all, the general environment in Russian-U.S. relations today is such that neither side trusts the other not to launch a large-scale government-sponsored cyber operation.

The incentive for both countries to work out at least some rules of cyberspace conduct lies not only in trying to prevent unwanted escalation but in pecuniary considerations. As ICTs' role in every aspect of human endeavor continues to grow, so does spending on cybersecurity, reaching over $120 billion worldwide, according to one recent estimate. Despite all this spending, the dangers of global cybercrime are growing as well, sometimes with negative implications for national security as governments themselves fall prey to ransom. For Russia and the U.S., as well as other countries, the cost of trying to keep up with cyber threats on their own could soon far outweigh that of compromising on potential regulations.

Thus, it is clear to me that Russia and the U.S. must engage in robust, ongoing dialogue to make cyberspace safer and more predictable. While tensions between the two countries might currently be too high for formal binding agreements, the sides must work to chip away at their sense of total mistrust and to inch toward cyber comity. Track 2 or 1.5 expert dialogue,

without preconditions, could precede actual negotiations between the two governments, providing each with a much-needed, in-depth understanding of the other's positions. Moscow and Washington could also resume confidence-building measures, such as sharing information on common threats or finding ways to work together on international cybercrimes that affect both parties; they should also seek ways to reveal to one another limited elements of their cyber postures and capabilities. If these two great powers can find a middle ground where rules are agreed upon, I believe the rest of the world could likely be persuaded to comply.

Cyber Bones of Contention in US-Russian Relations

Apart from the more recent political impediments to U.S.-Russian dialogue on the future of cyber norms and governance, much of the current deadlock results from the two countries' longer-term inability to understand each other's positions on ICTs, much less to reconcile them. The fault lines emerged as early as the 1990s when the U.S. became the center of an information revolution and the American private sector was a driving force behind the internet's spread around the world. Nowadays, the differences described below help explain why some of the cyber-related arguments that Moscow puts forward on the international stage and considers "peaceful" are seen as aggressive by the U.S. and other Western democracies. The major disagreements between Russia and the U.S. on cyber norms and security concern at least three major areas: the role of government in overseeing cyberspace; the militarization of cyberspace and the related applicability of existing international law; and the idea of legally binding treaties, including those that ban certain technologies, versus non-binding guidelines for how ICTs should be used. Certainly, the introduction of new U.S. sanctions as punishment against Russia in the wake of the SolarWinds breach has complicated matters even further.

The first essential difference between the Russian and U.S. positions lies in the respective roles of the state and private interests in the development and oversight of ICTs: More specifically, where Russia's approach to the cyber domain, like China's, aims for a sort of virtual border that keeps

out unwanted foreign influences and gives the government a great deal of leverage over the ICT sector, the U.S. encourages the free exchange of information and minimal regulation. Hence, Russian policy assumes a far broader scope of government responsibility and control in the cyber domain, in terms of both online content and ICT infrastructure. This includes state authority to collect personal data with minimal meaningful judicial oversight, to block or criminalize a much wider array of content than in the U.S. and to require service providers to aid in these efforts. Broadly speaking, the Russian government perceives individual freedoms in cyberspace as a threat and tends to use ICTs to try to limit its citizens' activities online. From a U.S. perspective, many of these measures seem excessively intrusive or heavy-handed and incompatible with American civil liberties. Moreover, the U.S. has long promoted a mix of governmental restraint and entrepreneurial initiative in developing the internet and related ICTs (recent antitrust concerns about Big Tech notwithstanding). Many Western liberal democracies today espouse similar policies. In short, though the U.S. government faces its own balancing act between security and civil liberties, and has its own symbiotic relationship with the private IT sector, Russia's approach to ICT-related policies generally gives the state far more regulatory and coercive power than in the U.S.

A related difference lies in the two sides' preferences for internet governance—"sovereign" and state-controlled (Moscow's) versus "global" and less dependent on governments (Washington's). Since the late 1990s Russia has tried to convince the international community that U.S. ICT policies unfairly benefit American private companies and that cyberspace would be safer if rules for internet governance were hashed out at the United Nations instead. There and elsewhere, Moscow has actively advocated sovereign cyber norms, suggesting that national governments should enhance legal control over cyberspace, including over the information available via ICTs. Although this approach runs counter to the borderless, global nature of the internet and its flows of information, Moscow has since found supporters of its position at the U.N. and other international fora, as discussed in more detail below. Washington, on the contrary, supports giving the reins of internet governance to multilateral institutions or private groups that would operate with relatively little government input.

Another major difference concerns publicly declared positions on military applications of cyber capabilities: Russia's official position has long been that the military use of cyber technology constitutes irresponsible state behavior and should be prohibited by international law; the U.S., on the contrary, acknowledges cyber instruments as a legitimate part of nations' military tool box for both defense and offense. This difference, too, has its roots in the 1990s. In the decade following the Soviet collapse, Russia's military might relative to that of the United States declined precipitously. Since no nations at the time had any significant military cyber units, it made sense for Moscow to adopt the view that ICTs should not be used as offensive weapons by armed forces, thus, presumably, safeguarding itself against the development of cyber capabilities by its adversaries. Russia has consistently stuck to this position in its official public pronouncements and promoted it in international relations, even after the creation of so-called cyber troops within its military (more on which below). Russia's current ambassador to Washington, Anatoly Antonov, reiterated this position in October 2020, following new U.S. sanctions against a Russian institute allegedly connected to a potentially life-threatening cyberattack against Saudi Arabia: "Russia, unlike the United States, does not conduct offensive operations in the cyber sphere," he said, adding that "malignant activities in the information space run counter to the principles of our foreign policy, national interests and understanding of inter-state relations." As on offshoot of this position, Moscow has also long been skeptical about the application of certain existing international laws to cyberspace, arguing it would legitimize the military use of ICTs. The U.S., meanwhile, believes that Russia, along with China, poses "the greatest [cyber] espionage and cyberattack threats" to the U.S. globally. Moreover, the U.S. openly admits the development of national military cyber capabilities and, in 2017, elevated its Cyber Command to the status of a unified combatant command—a move that Moscow almost certainly saw as threatening.

Finally, while Russia has voiced some objections to the application of existing international law to cyberspace, it has long called for new legally binding international cyber norms, a position reiterated in March 2021 by the Russian president; the U.S., on the contrary, sees this as excessive regulation and has preferred to promote non-binding norms that regulate the use and effects of ICTs. Thus, the U.S. perspective on "war and peace," as

described recently by senior cyber diplomat Michele Markoff, is "not that the technology itself is bad or good, but that it's states' use of technology and the effects that use … can have that's troubling." In Moscow's pursuit of legally binding treaties on cyber relations Washington sees an attempt to circumscribe certain ICTs, according to Markoff. Indeed, as early as 1998, Russia introduced a U.N. resolution expressing "concern" that certain ICTs "can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security."

If all of these differences made dialogue difficult enough, the sweeping U.S. sanctions introduced on April 15, 2021, make the prospects dimmer still, in my view. First of all, there do not seem to be any clear conditions for getting the sanctions lifted, giving Russia no incentive to engage with Washington, much less to modify its behavior. Second, the sanctions affect not only individuals and organizations but sovereign debt. These two factors raise the specter that the sanctions can be used as a cudgel against Russia well after the alleged offenses have been discontinued or remedied—much like the infamous Jackson-Vanik amendment. Third, the connection between the sanctions and the SolarWinds hack is somewhat tenuous: Though the U.S. government has accused Russia's foreign intelligence service, known as the SVR, of carrying out the hack, the Treasury Department's announcement said little about the extent or nature of the damage—noting only that "the SVR has put at risk the global technology supply chain by allowing malware to be installed on the machines of tens of thousands of SolarWinds' customers" and that fully remedying the intrusion "will cost businesses and consumers in the United States and worldwide millions of dollars." Finally, the sanctions do not seem entirely fair: Though they were said to punish unspecified "hack-and-leak operations targeting elections in the United States," the U.S. intelligence community has assessed with "high confidence" both that Russia's actions during the 2020 election cycle were less intrusive than in 2016 and that Iran conducted a covert influence campaign comparable to Russia's. Taken together, I fear these circumstances may greatly reduce Russia's appetite for dialogue on cyber issues that could affect both countries' vital interests.

Russia's Approach to Internet and Information Regulation: A Digital Iron Curtain?

Russia's cybersecurity policies are consistent with its broader political and legal traditions. These include domestic policies that are paternalistic, socially conservative and enforce collective identity. As opposed to the liberal tradition of individualism, Russian political culture prioritizes the interests of the state and its vision of society over the liberties and initiative of individual citizens. The executive branch of government wields more power, and has weaker checks and balances, than in Western democracies. And Russian policy still involves a great deal of government planning, similar to Soviet times, which makes the Russian economy uncompetitive vis-à-vis its Western counterparts.

As can be surmised from the section above, Russian state participation in the domestic cyber domain is far-reaching, with the government controlling not only technical aspects of ICTs but also paying a great deal of attention to content. This is partly reflected in the fact that the American term "cybersecurity" is often translated into Russian as "information security." (Indeed, upon its creation the cyber unit of Moscow's Defense Ministry was called "information-operations troops" and officially described as a counter-propaganda department.) In Russia the government holds the authority to designate information as "harmful" or "damaging"[19] and possesses the technical means to block access to such information. Although the U.S. has its own legislation limiting certain types of internet content, the range of restricted content is much narrower than in Russia and such regulations constantly meet with pushback from advocates of free speech and other civil liberties. Russian regulations about online content can be very broad. For example, in 2013 Russia criminalized content that offends the sensibilities of religious citizens and in 2019 passed legislation criminalizing content that insults the authorities. The latter was adopted along with the so-called "fake news law," which empowered the federal

19 This language can be found in legislation such as the 2010 federal law "On defending children from information harmful to their health and development" and the 2019 amendments to the federal law "On information, information technologies and protecting information" (a.k.a. the "fake news law" described below).

government to delete online information it deems inauthentic or misleading without court authorization.

Russia's cyber-related foreign policy initiatives are generally in line with these strict domestic regulations. Moreover, one of the government's priorities in its information policy is to ensure that audiences both in Russia and abroad get "reliable information" about Russia's policies and official positions. Both the latest strategic guidance issued by the Kremlin about international information security, approved April 12, 2021, and the most recent Information Security Doctrine,[20] published in 2016, do not focus on individuals, as did Russia's earliest cyberspace doctrine in 2000, but on national interests in the "information space." While much of the strategic "Foundations" document seeks to advance Moscow's vision of information security on the international stage, much of the 2016 doctrine seeks to increase Russian government control over content. According to the latter, one of the most serious threats to national security is the growing "information influence on the population of Russia…, first and foremost on young people, with the aim of eroding traditional Russian spiritual-moral values." Ensuring that all content conforms to Russian regulations—rather than ensuring the technical security of communications—stands out as the main focus of the document, which does not even mention the word "internet." The doctrine implicitly authorizes the government to regulate the activities of the media to promote favorable, pro-government coverage.[21] It also states that: "There is a trend among foreign media to publish an increasing number of materials containing biased assessments of state policy of the Russian Federation. Russian mass media often face blatant discrimination abroad, and Russian journalists are prevented from performing their professional duties."

Thus, people's access to alternative points of view in Russia is currently limited, given that most mainstream Russian media outlets, especially television, are either owned or controlled by the government. Online media platforms and social networks have become the chief sources of alternative information, with the number of people relying on them as their main news source rising from 15 percent in August 2009 to 81 percent in

20 An "unofficial" English translation of Russia's 2016 Information Security Doctrine is available on the Foreign Ministry's website.

21 See doctrine, points 33 and 35.

January 2021, according to Levada Center polls published in September 2020 and February 2021. The share of respondents who trust television news, according to the first of the two polls, declined from 79 percent in August 2009 to 48 percent in August 2020, while the share of those who trust online sources of news rose in the same period from 11 to 54 percent.[22]

Since 2016 Russia has passed laws significantly increasing state control over the internet. These were a response not only to people's increased reliance on online news but to simmering domestic political tensions and to growing international frictions in the wake of the 2014 Ukraine crisis. Moscow casts these measures as defensive. In December 2018 the State Duma, parliament's lower house, introduced legislation making various online activities unlawful. The first law, already mentioned above, focused on insulting "the society, state, official state symbols, Constitution and agencies exercising state power in the Russian Federation." Another set of amendments—the aforementioned fake-news legislation—lays out punishments for deliberately sharing via mass media or the internet "inaccurate socially significant information, disseminated under the guise of reliable messages, that creates a threat of causing harm to the life and (or) health of citizens, [or] property, a threat of mass violation of public order and (or) public safety or a threat of interfering with or stopping the functioning of essential services." In 2019, the government passed its most sweeping regulation: Called "Russia's sovereign internet act," it puts nearly all telecommunication infrastructure under government control and could potentially disconnect Russia's part of cyberspace from the rest of the world's.

Together, all the legislation that prevents Russian citizens from accessing foreign information—and augments the authorities of Russia's special services and law enforcement agencies in the cyber realm—forms a kind of digital version of the infamous Soviet Iron Curtain. That said, the metaphorical curtain seems to have more holes now than it did then. One vivid example concerns the state's dealings with the messaging platform Twitter: For years, Russian authorities have been trying in vain to force the company to store Russian users' data on servers inside Russia, as mandated by

22 The 54 percent includes 7 percent who said their most trustworthy news source was the encrypted chat service Telegram, which was included in the polls as a separate category in January 2020.

a 2015 law; this battle culminated in 2020 in fines that were large by local measures but barely dented Twitter's budget. Even bigger fines were levied in April 2021 because the state communications watchdog, Roskomnadzor, says Twitter has been unwilling to remove objectionable content. The most radical technological intervention began in March 2021 when Roskomnadzor slowed down access to Twitter—a move that reportedly has affected Russian users very unevenly across the country's 80-plus constituent territories and triggered inadvertent slowdowns of unrelated but widely used domains such as microsoft.com. This experience, as well as Russia's even less successful attempt to block the Telegram messaging app, suggests that bans and prohibitions are not the most effective ways to pursue cybersecurity.

Moscow's fears concerning unchecked flows of information online and its policies of enhanced state control over data and ICT infrastructure create something of a vicious cycle, in my view: As officials wall off Russia's piece of cyberspace, the country becomes likelier to self-isolate from Western civilization, thus reducing chances for dialogue; meanwhile, Moscow's tightening control over information contributes to a negative perception of Russia in the eyes of more liberal Western societies, where views on the country and its government's policies are already sometimes skewed by sensationalism, ignorance or other factors.

Nonetheless, Russia takes its concept of international information security and the promotion of that concept worldwide very seriously. In 2011, Russia proposed that all countries adopt a Convention on International Information Security reflecting Moscow's position that such security can be ensured only by strong government control. At the end of 2019, President Vladimir Putin approved the creation of a new Foreign Ministry department focused exclusively on promoting international information security. It is led by Andrey Krutskikh, a prominent diplomat known for representing Russia's position on cyber issues at the U.N., which Russia still sees as the main platform for promoting its vision. (This is another example of Russia's policies following in Soviet footsteps—trying to preserve global influence through international institutions created during the Cold War, when Moscow had much more influence, and where it still has a prominent seat at the table.) In April 2021 the Kremlin approved its latest

strategic guidance on cyber policy, called "Foundations of State Policy in the Field of International Information Security," which once again affirmed a central role for the state and its priorities.

That said, while Russian diplomats have worked to multilateralize Russian proposals, Krutskikh seems to realize the importance of building mutual understanding with the United States on cyber issues. In a March 2019 op-ed for Kommersant, a Russian news daily, he wrote that "today, just as 50 years ago, we talk about preventing a cyber incident from escalating into a full-scale military conflict between Russia and the United States. If the established emergency 'hotlines' bolstered with dialogue between experts stall for political reasons, we will face the risk of another Cuban Missile Crisis, only this time it will be triggered by information and communication technologies, not warheads, and events will unfold in a matter of minutes, leaving little time for both sides to make their decisions." Despite the Foreign Ministry's public position on U.S. accusations of cyber malfeasance, I believe, perhaps optimistically, that Moscow's diplomats realize the gravity of the accusations Russia faces from the West—particularly concerning its alleged election interference—and intend to work with Western countries on increasing mutual understanding and raising predictability. The surprising compromises described in the "diplomatic measures" section below support this view.

Russian Threat Perception Vis-à-Vis US Cyber Priorities

Cyberspace has obviously become a domain of confrontation between Russia and the United States. Both countries use different ICT instruments that, in the context of generally strained relations, further ramp up bilateral tensions. While the topic that seems to dominate U.S.-Russian relations in this sphere today is Russia's alleged meddling in U.S. domestic politics and, more recently, the SolarWinds breach and the USAID spear-phishing hack, there are multiple, overlapping fields of cyber contention where Moscow occasionally interprets, or misinterprets, American positions as hostility. These include not only the development of ICTs for military use but unchecked flows of information—which Moscow sometimes regards as

a means of U.S. interference in its domestic affairs—as well as commercial activity and internet governance.

In contrast to Russia's cyber policies, the U.S. approach to ICTs, as noted before, emphasizes limited government involvement and individual liberties, with "the free flow of ideas and information" seen as valuable in and of itself. Leaders in Moscow, however, view this borderless version of freedom of speech as a challenge to Russia's "spiritual-moral values" and as a means for the U.S. to wield soft power through instruments such as media, educational programs and scholarly exchanges. Seeing in these a threat to Russia's sovereignty and national interests, Moscow tries to limit Russian citizens' exposure to such influence on Russian soil. Moscow perceives some of the related U.S. policies as a form of information operations and/or interference in Russia's domestic affairs, especially as they were once accompanied by aid to Russian NGOs that challenged the authorities' hold on power. A related threat to Russia's cyber sovereignty, in Moscow's view, lies in the U.S. policy of reducing government involvement in global internet governance, which culminated in 2016 in the transfer of domain-name management to the private sector. (Russia is reportedly attempting to "supplant" the private group now in charge of internet addresses, ICANN, through a plan to take over a U.N. telecommunications group.)

Russian decision-makers also regard U.S. commercial ICT superiority both as a threat to their vision of sovereign cyber space and as unfair competition. About half the world's top 20 technology companies are U.S.-based. Moscow has launched anti-monopoly probes into Apple and Google, as have some Western countries—although Russian ICT companies are uncompetitive for many other reasons, in my view. Russia has furthermore tried to gain greater control over the content available to Russians via the U.S. ICT sector. These efforts have included requirements, as mentioned above, to process Russians' personal data using servers within Russian borders and also to preinstall Russian software on devices sold in Russia. In this year's strategic guidance, the Kremlin went so far as to say that "certain states'" use of their "technological domination" of global cyberspace poses a threat to Russia through the monopolization of ICT markets and restrictions on other states' access to cutting-edge technologies and other cyber-related resources.

Unsurprisingly, another major source of anxiety for Russian leaders lies in U.S. military cyber policy. While many details may be classified, Washington makes no secret of working on military cyber capabilities as such. Moreover, after the Trump administration's elevation of Cyber Command, the latter's emphasis shifted from Obama-era deterrence to a more proactive stance, including new authorities to conduct offensive or preemptive operations. The latest U.S. cyber "command vision" builds on the military's concept of "defending forward" by introducing the notion of persistent engagement—continuous cyber operations "below the threshold of armed conflict … [that] can influence the calculations of our adversaries, deter aggression and clarify the distinction between acceptable and unacceptable behavior in cyberspace." The U.S. sees this as essentially mirroring the activities of its major adversaries in cyberspace—Russia, China, Iran and North Korea. Washington believes that these countries conduct constant cyber operations and cyberattacks against U.S. infrastructure and institutions, inflicting some damage, though thus far not enough to provoke U.S. retaliation by military force. As then-Secretary of Defense Mark Esper said about cybersecurity in 2019: "Defending forward allows us to disrupt threats at the initial source before they reach our networks and systems. To do this, we must be in a position to continuously compete with the ongoing campaigns being waged against the United States."

This U.S. stance puts Russia in a tricky position: In Moscow's narrative, governments should not be developing offensive cyber capabilities but should instead be responsible for ensuring that ICTs are not used as instruments of aggression. Russia insists that it stands against the very idea of weaponizing information and, in public, denies accusations that it has condoned or executed state-backed cyberattacks or information operations. While such denials may seem unconvincing to Western audiences, they have significant traction in Russia itself (see poll figures below). Moscow's pacifist public position also means that other countries' open development of military cyber capabilities is almost certainly construed in Russia as a declaration of hostile intentions or a source of potential conflict. Russian Deputy Foreign Minister Sergei Ryabkov has even complained that U.S. accusations of "so-called malicious activity in cyberspace" by Moscow are "a manifestation of Washington's readiness to continuously lower the threshold for using nuclear weapons."

Finally, it is worth noting that these Russian threat perceptions are not limited to the halls of power. According to a 2018 Pew survey, 85 percent of Russians think the U.S. government "interferes in the domestic affairs of other countries," while fewer than half of Russians (45 percent) believe their government does the same; only 15 percent believe that the Russian government tried to influence the United States' 2016 presidential contest. This contrasts sharply with U.S. public opinion: According to one May 2019 poll, 73 percent of Americans believed Russia had "definitely" or "probably" interfered in the 2016 presidential election, and 60 percent felt that "the U.S. is not doing enough to stop Russian interference in the American electoral system."

Potential Basis for Cooperation

Despite the miserable state of bilateral relations today, and 20-plus years of U.S.-Russian disagreement about approaches to regulating cyber activity, both sides clearly understand the need for compromise and rules of the road in cyberspace and have achieved some impressive successes in bringing their positions closer together—even in the past few years. The most significant breakthrough of this sort came in March 2021 in the form of a U.N. report reaffirming 11 voluntary norms (see Appendix 1) for responsible state behavior in cyberspace and supported unanimously by 193 states, including both Russia and the U.S. This achievement was all the more noteworthy because as recently as 2018 Moscow and Washington had sponsored dueling U.N. resolutions on cyber norms linked by some experts to "irreconcilable differences in the way … Russia and the United States viewed cyberspace as a domain for conflict." These differences will certainly persist for a long time and are manifest both in Russia's latest strategic cyber document and in continued cyber-related tensions between Russia and the U.S. But diplomats' ability to quash some of the biggest differences between Moscow and Washington, temporarily at least, gives some grounds for hope.

The authors of the 2021 U.N. report on cyber norms, described in more detail below, managed to build on earlier successes: The basic principles reaffirmed in the report were developed in 2015, after the crisis in Ukraine

was well underway, by a U.N. group of government experts (GGE) from 20 countries, including both Russia and the U.S. Prior to the Ukraine crisis there had been progress in bilateral talks on cybersecurity as well. In 2013, on the sidelines of a G8 summit in Ireland, presidents Putin and Barack Obama signed an agreement aimed at building confidence and transparency between the two nations' cybersecurity efforts. The agreement affirmed that the sides saw cooperation in the ICT field as "essential to safeguarding the security of our countries," and was mainly aimed at creating better information-sharing mechanisms and a bilateral working group on cyber threats to international security. A few months later, these cyber efforts were mentioned in a U.S. government report on presidential working groups as one of the most promising fields of bilateral cooperation. Unfortunately, the dramatic deterioration in diplomatic relations between the two countries since 2015 has put many of these confidence-building measures on ice and more generally cut down opportunities for bilateral initiatives in the cyber realm.

As suggested above, there is no doubt that the U.N. consensus reached in March 2021 is a fragile one. The Kremlin's latest strategic guidance on "international information policy" was approved a month after the OEWG report was released, once again emphasizing governments' role in maintaining cybersecurity, while giving short shrift to the interests of individuals and civil society. Moreover, the document highlights two new threats that seem to reflect Russian-U.S. cyber tensions: "computer attacks against states' information resources, including critical information infrastructure," and the "technological domination" of global cyberspace described in the previous section. In a throwback to the Cold War, some U.N. member states, as demonstrated below, have been taking sides, supporting either Moscow or Washington on some of the wedge issues.

Nonetheless, despite the significant differences between Russian and U.S. positions on cyberspace and the ongoing bilateral tensions, including the latest round of sanctions, there are still joint measures the two can undertake to, at the very least, keep lines of communication as open as possible and thereby reduce the risk of inadvertent cyber-related escalation. The key realistic goal for each country should be to better understand the other side's position on cyber policy and to more clearly articulate its own—not

always publicly. A top focus of these discussions should be the clarification of red lines and triggers for kinetic retaliation. The most promising avenues for achieving this, in my view, include three overlapping, complementary areas of discussion, initially in a Track 2 or 1.5 format: bilateral talks building on the legacy of U.S.-Russian arms control to counter threats posed by national military cyber capabilities; bilateral and/or multilateral talks on possible norms for state behavior in the cyber domain; and bilateral and/or multilateral cooperation in fields where the two sides' cyber interests converge, for example in combatting materially driven cybercrime, cyber terrorism and other forms of non-state cyber aggression. Part of this effort, as noted above, will involve distinguishing between cyber threats that the two governments can combat jointly and those that the governments pose to each other. To make even modest progress toward greater predictability, both countries will likely have to recalibrate their public positions: Russia will, at the very least, have to go beyond an oblique acknowledgement that military cyber weapons exist as such and be willing to actually discuss ICTs in a military context, while the U.S. administration will need to tone down its harsh rhetoric, including headline-grabbing but unproven allegations against Russia's leadership, and to allow open-ended dialogue instead of cutting off channels of communication.

Possible bilateral cooperation on cyber 'arms control'

The history of U.S.-Soviet/U.S.-Russian nuclear arms control inspires both optimism and a sense of urgency about managing inter-state contention in the cyber domain: The Cold War-era foes' successful track record of arms control agreements suggests that even the most sensitive areas of national security can become topics of negotiation between adversaries when both sides recognize that the status quo is untenably dangerous, while incidents like the Cuban Missile Crisis highlight the existential risks of escalation. It helps, too, that the Biden administration takes arms control seriously, even amid dismally poor relations. While it is unlikely that the two sides can conclude any binding cyber agreements in the foreseeable future, even regular, candid consultations will help relieve some of the bilateral tensions in this area. These tensions, after all, are exacerbated not just by differences in U.S. and Russian positions on the military use of cyber technologies but

by the lack of dialogue, mutual misperceptions and a seeming inability to acknowledge the other side's priorities and interests. As noted at the beginning of this paper, I believe progress on this front will require separating military cyber issues from other ICT-related topics. This would allow the two sides to address major risks to their national security without the extra baggage of highly politicized but ultimately lower-stakes questions like interference in domestic affairs. While gray areas, including questions related to espionage, will remain for years to come, even preliminary bilateral agreement on a very limited set of issues—such as red lines for military retaliation—could contribute considerably to transparency, predictability and thus global security.

To modern observers, U.S.-Soviet arms control seems like a given, but the early rounds of talks were filled with rancor, mistrust and no guarantees of success—much like bilateral cybersecurity talks would be today. The 1963 Limited Nuclear Test Ban Treaty, for example, took eight years to negotiate, with Moscow deeply hesitant about allowing verification inspections. One former intelligence official noted in conversation recently that weapons programs were so classified that, during one set of early arms control talks in Geneva, Soviet officers were supposedly hesitant to discuss certain aspects in front of Soviet diplomats because the latter had not previously been privy to all the relevant details. A former CIA officer said in 2021 that he could easily envision a similar scenario unfolding between U.S. intelligence officials and diplomats at cyber talks. Nonetheless, even during the Cold War, Washington and Moscow were able—through a mix of skilled diplomacy, prioritization, selective information sharing, technical expertise, patience and luck—to prevent their contention on the world stage from exploding into cataclysmic conflict. That experience must be built upon in pursuing cybersecurity. Swift extension of the New START Treaty in February 2021 was a promising development, which Moscow initially welcomed as a window of opportunity for constructive dialogue on a broader set of issues.

As with traditional arms control talks, a chief goal of U.S.-Russian cyber negotiations would be to prevent escalation—in this case, escalation to the use of military or other kinetic force. This prospect seems to be of concern to decision makers on both sides and, in my view, justifies considering

cyber issues within the broader context of U.S.-Russian tensions and strategic stability. Cyber aspects of arms control, however, have not made it onto the Russian-American agenda in sufficient measure—largely due to the incompatibility of the two sides' stances on military use of ICTs.

In addition to the differences described in detail above, it is also clear that both sides will want to retain flexibility in the areas where military operations and ICTs overlap—creating additional ambiguity and anxiety. In September 2020, the Defense Department's principal director for cyber policy, Madeline Mortelmans, made three pertinent points about this, presumably expressing the U.S. view: "A cyber operation can constitute an act of war"; an attack, cyber or otherwise, is defined by "the effects that are caused, rather than the means by which they are achieved"; and "a cyberattack does not necessarily require a cyber response." Russia, meanwhile, has officially disavowed the military use of ICTs, but has repeatedly expressed concerns about cyber-related "threats to … global security and to individual countries" and, as noted earlier, has officially created "information-operation troops" within its military. Defense Minister Sergei Shoigu and some experts have implied that these troops would be defensive in nature, with a focus on countering propaganda and other malicious foreign activities. (Washington likely views this position as disingenuous.) Neither country, moreover, specifies how cyber defense is different from cyber offense; indeed, like cyber espionage and the groundwork for cyberattacks, the two are often difficult to disentangle for technological reasons.

It is my hope that by focusing separately on the military and non-military aspects of cyber talks Russia and the U.S. can mitigate a major risk to their national security—namely, an escalation to war triggered by a state-sponsored cyberattack—without getting bogged down by less critical but more controversial issues. The latter include not just mutual allegations of interference in each other's domestic affairs but reported intrusions into critical infrastructure by both sides. The military track of such talks could focus on determining the relevant issues to be discussed and, eventually, the "red lines" that cannot be crossed—for example, any sort of breach of nuclear command and control systems. In a best-case scenario, candid talks in this area could lead to progress in other areas of cybersecurity and, in any case, such negotiations seem critical for understanding each other's priorities,

increasing predictability and lowering the risk of unwanted conflict. Obviously, for this to happen, Moscow will have to set aside its long-standing policy of declining to discuss cybersecurity in a military context; the U.S., in turn, will have to tone down its rhetoric, give more thoughtful consideration to the effectiveness of sanctions and be more open to dialogue without preconditions.

Unless Russia and the U.S. find some mutually acceptable mode of candid dialogue on cybersecurity, the atmosphere of ambiguity, non-transparency and fear of retaliation threatens to make decision makers in both countries jumpy, thus raising the risk of inadvertent conflict. The sphere of military cyber technology is classified for obvious reasons, but excessive secrecy raises additional concerns and stokes worst-case-scenario military planning in both countries. Of particular concern is the lack of clarity about retaliation on both sides. In the case of Russia, the highly classified nature of its cyber strategies makes it unclear which cyberattacks Moscow would consider an act of war and whether it would retaliate or how. On the U.S. side, more information about national cyber strategies is publicly available than in Russia, but ambiguity persists on the question of retaliation. According to its recent vision for achieving cyberspace superiority, U.S. Cyber Command considers Russia's persistent engagement in the cyber domain to be aggression "below the threshold of armed conflict." It is not clear to me where the U.S. sees that threshold, but such language suggests there *is* a red line—e.g., that the U.S. military differentiates between a cyberattack that triggers a kinetic military response and one that does not. Markoff, the U.S. cyber diplomat, has said there must be "lethality" for the threshold to be crossed. The CYBERCOM document, meanwhile, suggests that some U.S. officials consider the current threshold too high, saying: "We cede our freedom of action with lengthy approval processes that delay U.S. responses or set a very high threshold for responding to malicious cyber activities." It is no wonder that, in the current atmosphere, neither Moscow nor Washington trusts the other's declared peaceful intentions.

The goals of military-track cyber talks should, in my view, be largely definitional, tackling at least three sets of questions: (1) What is a cyber weapon? Can it be subject to international law, including agreed-upon classifications, rules of engagement, restrictions on proliferation and other

terms? Discussions could consider the possibilities of export controls and controlling or preventing a cyber arms race. (2) What is a cyberattack? Specifically, the sides have to zero in on the definition of a state-sponsored military cyberattack, which would require a comprehensive view of the tools used, the sources/vectors of attack, motives and targets, as well as the damage inflicted. If the threshold for designating a cyber operation as an attack is low, this would suggest that even limited use of cyber weapons could spark retaliation with kinetic weapons; theoretically, as the level of trust rises, so will the threshold. (3) On a related note, what are the red lines that would trigger military retaliation if crossed?

To sum up, the "arms control" logic described above implies that, within the military track for cyber talks, Moscow and Washington discuss only the threats they pose to each other. Ideally, they would agree on a detailed protocol for attributing cyberattacks. In cases when both sides have concluded that an attack was not state-sponsored, it should be regarded as a cybercrime and addressed through a cooperative joint effort (more on which below). Various cyber incidents will continue to fall into a gray area, but the designation of one "insulated" high-stakes track for talks will hopefully open up opportunities to address the less black-and-white issues down the road in a calmer setting.

Another important consideration in this regard is that Russia's current position regarding escalation in a cyber context emphasizes preventing military escalation *in cyberspace*. I believe it would be far more constructive to direct bilateral efforts at preventing military escalation *of any sort*, thus enabling the sides to discuss cybersecurity in the context of arms control. This logic seems more compatible with the U.S. view described by both Markoff and Mortelmans, wherein cyber tools are but one means among many that states (and non-state actors) use in pursuing their larger goals, rather than a siloed category of instruments that exist only in the cyber domain.

Bilateral efforts are also worth pursuing because they would prove as important as multilateral talks in working out global norms of responsible behavior in the cyber domain. Precisely because the Russian and U.S. stances on cyber policy are so polarized, and because two international

camps have been gathering around these poles, even limited bilateral consensus could contribute hugely to advances in multilateral agreement.

Finally, it is worth noting that one aspect of traditional arms control that seems virtually inapplicable to the cyber domain, in my view, is deterrence. This stems from differences between nuclear and cyber weapons in at least four areas: quantity, clarity of definitions, cost/symmetry and attribution.

a. In terms of quantity, the goal of nuclear deterrence has been to prevent even one nuclear attack by developing capabilities for an obliterating retaliatory strike; cyberattacks, meanwhile, occur on a daily basis and their volume is astounding. The Pentagon alone reportedly thwarts some 36 million email breach attempts a day. Even when cyber exploits are used as weapons against an adversary, there are endless levels of damage they can do, so there can be no cyber equivalent of Robert McNamara's famous doctrine of "mutually assured destruction."

b. As far as definitions go, unlike missiles and nuclear warheads, cyber weapons and other forms of aggression in cyberspace do not have clear, agreed-upon definitions, as noted before. Russian and U.S. cyber potentials are classified (Russia's probably to a greater extent than America's), which can distort perceptions of the other's capabilities.

c. Furthermore, unlike nuclear arms, cyber tools are relatively cheap and used for many different purposes by many different actors—in and out of government and the military. Even consumer electronics may be used to inflict damage. If nuclear deterrence was based in part on the idea of parity in the number of weapons, this concept cannot apply to cyber contention, which is marked by an asymmetry of threats, capabilities and vulnerabilities.

d. Finally, experts agree that cyberattacks are notoriously difficult to attribute. There is no missile to detect and no tracking system to show the origins of an attack. Even in cases when Washington officially accuses Russian government actors of hacking, only a small part of the evidence becomes available for public scrutiny. Also, the SolarWinds case has demonstrated, once again, that it can

be difficult to distinguish groundwork for cyberattacks from cyber espionage, as both require breaching and familiarizing oneself with adversaries' networks.

Thus, although there have been attempts to develop a cyber deterrence paradigm, the differences between nuclear and cyber weapons necessitate very different approaches.

Diplomatic measures aimed at regulating cyberspace as a global domain

If Russia and the U.S. start negotiating certain aspects of cybersecurity as part of the bilateral arms control agenda, thus transferring them to the military, diplomats would be freer to focus on other issues on the non-domestic cyber agenda—specifically, on working out international norms of state behavior in cyberspace. These two tracks should be seen as complementary and, at times, overlapping, not mutually exclusive, and thus do require an inter-agency approach. One general difference between them, in my view, is that the U.S.-Russian arms control track on cybersecurity should address only threats that the two states pose to one another, with the larger goal of avoiding escalation to or beyond the threshold of armed conflict; the diplomatic track, meanwhile, would focus on working out cyber rules of the road that—while keeping the two sides as far from that threshold as possible—can be applied more broadly and also involve joint cooperative measures against cyberthreats that they have in common, whether from third states or non-state actors, including those operating on the territory of Russia and the United States. Success in this area will require overcoming not just the divides between Moscow and Washington but between larger groups of countries coalescing around their respective approaches to managing cyberspace.

All the post-2014 progress on cyber norms mentioned at the beginning of this section, and described in greater detail below, has come about through diplomacy. Hence, I am convinced that diplomatic efforts on cyber security should continue. Moreover, they need to be bilateral as well as multilateral, in my view, since the latter will always yield results that are more watered

down by virtue of the larger number of participants and, consequently, more interests to be balanced.

Both of the recent U.N. documents reflecting consensus on cyber norms required deft diplomacy and compromises on both sides. In the 2021 report, produced by a U.N. body called an open-ended working group (OEWG), Russia seems to have shifted emphasis away from some of the ideas that had drawn so much opposition from the U.S. and its allies three years earlier—like "sovereign internet" and "information security"—to cybersecurity in the American sense (focusing less on content and more on ICT-related infrastructure); the U.S., meanwhile, agreed to allow dissenting opinions—rather than insisting on full consensus—by incorporating language that it sees, in Markoff's words, as "retrograde" and "authoritarian" into a chair's summary accompanying the report. Several months later, the OEWG consensus was reaffirmed in a new GGE report that experts had feared might lead to another split between Moscow and Washington. Markoff, who negotiated on the United States' behalf, lauded the 2021 GGE report as a "substantial new body of guidance" and applauded its authors for their "extraordinary willingness to bridge differences in order to reach consensus." Likewise, after the 2015 GGE report had been issued, Vladislav Sherstyuk, a cybersecurity expert and advisor to the head of Russia's Security Council, called the consensus "historic," while an American cybersecurity reporter called it "a breakthrough for U.S. diplomats." (Earlier U.N. GGE consensus reports had also been issued in 2013 and 2010, but they were less detailed and emerged amid the relative calm of the Obama-era "reset" in Russian-U.S. relations.)

At the same time, it is important to remember that the United Nations has been a key battleground for Russian-American disagreements on cyber norms since the late 1990s and the 2017-2018 rift over these norms divided member states into two international coalitions on opposite sides—one gathering around Russia, the other around the United States. And even though both Russia and the U.S. declare a commitment to the peaceful use of ICTs and encourage the international community to avoid such coalitions, it is clear that the world is getting more and more divided on two competing approaches to managing cyberspace, with Western democracies on one side and, on the other, Russia and China plus some other Asian as

well as African nations. The table below, first published in the Riddle in 2020, demonstrates this divide, which reflects differences both in technological infrastructure and in approaches to cyber regulations and internet governance. The table contains the average of key U.N. ICT development indices, World Bank infrastructure indicators and Freedom House's Global Freedom rating among the cosponsors of the competing resolutions proposed by Russia and the U.S. in 2018 and 2020. It is clear that the countries who supported Russia's resolutions are much less technologically advanced and politically less integrated into the digital world than supporters of the U.S. resolutions. There seems to be a clear borderline between the nations that pursue strong government control similar to Russia's "sovereign internet" or China's "Great Firewall" and those that promote freedom of speech and a more democratic internet. (Though this year's OEWG consensus report has softened these divisions, it certainly hasn't eradicated them. Some hurdles will need to be cleared in the near term, according to Markoff: In May 2021 a U.N. GGE that came to support the U.S. position in 2018 will be issuing its own document on norms and it is not yet clear whether Russia will sign on considering the success of the OEWG report, which involved 193 countries to the latest GGE's 25.)

	2018		2020	
	Resolution sponsored by Russia	**Resolution sponsored by the U.S.**	**Resolution sponsored by Russia**	**Resolution sponsored by the U.S.**
EGDI - E-Government Development Index	0.44	0.79	0.54	0.80
OSI - Online Service Index	0.44	0.83	0.52	0.77
TII - Telecommunications Infrastructure Index	0.29	0.67	0.46	0.78
HCI - Human Capital Index	0.62	0.86	0.69	0.85
EPI - E-participation index	0.42	0.85	0.50	0.80
Fixed telephone subscriptions (per 100 inhabitants)	10.94	31.27	9.02	27.53
Mobile cellular subscriptions (per 100 inhabitants)	88.58	120.88	97.04	120.64
Fixed broadband subscriptions (per 100 inhabitants)	7.86	31.82	7.97	30.59
Global Freedom Scores	31.32	89.14	19.88	85.04

In a best-case scenario, sustained, focused diplomatic work may eventually lead to an atmosphere were a case like the SolarWinds breach (and perhaps the USAID-spoof phishing campaign reported in May 2021) would either not have happened or not have led to nearly so much talk of retaliation and "acts of war." In addition to distinguishing between various forms of cyber operations and tools, Russia and the U.S. should strive to agree on acceptable boundaries for cyber espionage and to develop protocols for attributing cyber operations. If an operation were deemed to be an attack and attributed, under such a protocol, to a state-sponsored actor, the countries could leave the problem to the military to discuss as an intentional act by one state against the other. If the perpetrator proved to be a non-state actor, the countries could reasonably share information about the attack.

Cooperation on joint threats

Russia and the U.S. have long faced common threats that involve a cyber component, including organized crime, terrorism, financial fraud, violations of intellectual property rights, economic espionage and drug trafficking. And just as cyber aspects of military contention should be discussed, in my view, as part of a larger dialogue on military tensions, so too should these shared threats be prioritized in bilateral relations without thinking that the related cybersecurity issues can be solved separately from subject-specific dialogue. Perhaps such an approach would help depoliticize talks on cybersecurity, leading to more constructive negotiations.

One logical source to consult for bilateral consensus building in this area would be the list of 11 norms reaffirmed in March 2021. Of these, the one that I believe could prove most fruitful concerns working together against crime: "States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect." While bilateral cooperation against materially driven cybercrime has suffered setbacks in recent years, I believe it could be reinvigorated if the crime-fighting track is separated from other issues and depoliticized. The countries could discuss different instruments to jointly conduct

investigations, prosecution and possibly extradition of cybercriminals. Such cooperative measures could go beyond cyberspace, involving legal cooperation more generally, against organized crime or terrorist threats. This, in turn, may help build goodwill and trust.

If bilateral cooperation against cybercrime were more robust, the Colonial Pipeline ransomware attack of May 2021 could have been a good opportunity to put it into action. First of all, though the hack has tentatively been attributed to non-state actors with some presence in Russia, U.S. officials have not blamed Moscow. President Joe Biden has repeatedly emphasized that "there is no evidence … from our intelligence people that Russia is involved." Independent cybersecurity companies also have not attributed the attack to the Russian government. Second, based on Russia's earlier declarations, Moscow cannot be opposed to cooperating with Washington against such threats. Cybersecurity will clearly be on the agenda during the June 2021 meeting between Putin and Biden. Approaching the issue from this angle may allow the two sides to ratchet down mutual accusations of domestic political interference and lay the groundwork for mutually beneficial cooperation instead.

One test for this line of thinking came in May 2021 when the U.N. Legal Affairs Committee began a Russia-initiated process for devising a new cybercrime instrument. Before the committee met, the U.S., according to Markoff, believed the proposed document was meant to "eclipse and potentially replace" the so-called Budapest Convention of the Council of Europe, which entered into force in 2004 as the only binding international treaty on cybercrime and has not been signed by Russia. Nonetheless, on May 26, 2021, the U.N. General Assembly unanimously passed a resolution titled "Countering the use of information and communications technologies for criminal purposes," which, according to the U.N. press office, Russia's representative described as a "very balanced and subtle compromise text" that Moscow had changed considerably in order to ensure broader support for the draft. Substantive work on the cybercrime convention is set to begin in January 2022 with a draft to be submitted for review by the 78th General Assembly in 2023.

Recent compromises notwithstanding, a high level of mistrust between Russia and the U.S. remains, so it is probably worth thinking about how to make cyber cooperation possible not only at a government level but beyond, involving stakeholders that have heretofore been sidelined but have a strong interest in cybersecurity—in particular the private ICT sector. On one hand, in recent years, U.S.-Russian mistrust has seeped into this sphere as well, with U.S. officials introducing measures against various private Russian tech and cybersecurity enterprises: Sanctions implemented in response to the SolarWinds breach, for example, targeted several private companies; the American operations of cybersecurity provider Kaspersky Labs, which U.S. officials suspect of being too close to the Kremlin, have been severely restricted since 2017; a senior executive at cyber forensics company Group IB was accused in 2014 of materially driven cybercrimes. And some U.S. companies, as noted above, are seen by Moscow as potential threats to Russian cyber sovereignty. On the other hand, nongovernment cyber forensics experts can theoretically brainstorm on best practices or cooperative measures—for attributing cybercrimes, for instance—without revealing sensitive information. One paradoxical episode that suggests such cooperation could be possible involves Group IB (which has defended its employee and has not been accused of wrongdoing itself): Late in 2020, the company wrote that a hacker with the nickname "fxmsp"—whose exploits it had detailed in a June 2020 report—had been selling access to SolarWinds software on the dark web back in 2017; a month after the Group IB report, the U.S. Department of Justice charged a citizen of Kazakhstan who had allegedly used the fxmsp persona for hacking hundreds of corporate networks worldwide.

A few more words on terminology

As implied above, a major impediment to progress toward cyber rules of the road is the large number of terms on which the two sides do not agree. In order to facilitate the development of bilateral confidence-building measures and, ideally, greater cooperation in areas such as combatting cybercrime, experts dispatched by Moscow and Washington will need to build consensus on some key terms, or at least furnish decisionmakers

with sufficient information about each country's positions and priorities to understand where the salient differences lie.

Attempts at creating a Russian-English cyber glossary have already been made but deserve to be expanded and updated. Perhaps the most significant bilateral effort to date came in 2011, and was expanded in 2013, by the U.S.-based EastWest Institute[23] and Russia's Information Security Institute. This glossary, however, was based on expert assessments, while it is also important, in my view, to include definitions from official government publications. The U.S. Department of Defense regularly publishes glossaries on all issues, including cyber. Russian government agencies have similar publications. There should also be several baskets of terms—for example, military, international cooperation and commercial. -

Apart from the three terms mentioned in the arms-control section above, the most pressing need for clarification, in my view, concerns the following:

- Aggression: What ICT-enabled actions can be qualified as aggression and could trigger retaliation? (Once the countries agree on that, political leaders can declare that they will refrain from cyber aggression for the purpose of achieving political goals.)
- Sovereignty: While this concept continues to be debated even among allies, there needs to be greater clarity on the extent to which ICTs and other cyber resources can be considered a national asset—subject to national laws—as opposed to part of an international domain.
- Offense and defense in cyberspace: How does one draw a line between offense and defense in cyberspace? Which military authorities are allowed to conduct offensive cyberattacks and defensive operations?
- Interference: Based on Russian and American mutual accusations of interference in domestic affairs, it is clear that the term is understood in very different ways.

23 As noted earlier, EastWest's programs on cyber issues were transferred early in 2021 to Observer Research Foundation America.

- War and peace: Clearly the state of relations between Russia and the U.S. cannot be qualified as war, at least at this point, but the number of hostile activities from both sides suggest it is not peace either. What is this intermediate state of adversarial relations, which one former CIA officer has termed a perpetual "ambient cyberconflict"?
- Escalation: What constitutes conflict escalation in cyberspace? What are the pathways of escalation? How can conflict move from the cyber to the physical domain? What are each country's relevant national interests and red lines?

Beyond terminology, some have suggested that a basis for bilateral cyber cooperation could be the Tallinn Manual—a 2013 examination of the applicability of international law to cyber warfare written by a NATO-convened group of experts and updated in 2017. This does not strike me as promising. First of all, the manual reflects some aspects of the general Western approach to cybersecurity policies that Russia rejects, as described above. Second, many of NATO's cybersecurity and military efforts are aimed against Russia specifically, which makes the manual a weak foundation for bilateral cooperation. Last but not least, the manual states that NATO's famous "Article 5" about collective defense should apply to cyberspace—a proposition to which Russia would never agree.

Conclusions and Recommendations

Due to extremely high levels of mutual mistrust and political "toxicity" at this point, it is highly unlikely that Russian and U.S. foreign policy decision-makers will manage to overcome the differences between the two sides and reach a formal agreement on cyber rules of the road in the foreseeable future. It also seems that Russian and American positions on several major cyber-related issues are so far apart that consensus is impossible. However, in the past, comparable obstacles did not prevent Russia and the U.S. from engaging in dialogue and eventually resolving some of the thorniest issues in bilateral relations.

Now, too, it is critical to seek mutual understanding about each state's cyber policies and priorities, including how each sees its vital national

interests beyond the cyber domain. The most promising vehicle for such efforts at this time is Track 2 or 1.5 expert dialogue, ideally without preconditions. Russian and U.S. government efforts should generally be aimed at reaching greater transparency and predictability in cyber operations and greater resiliency and stability in cyberspace.

As a practical means of achieving this, I believe Russia and the U.S. should divide the existing mass of cybersecurity issues into two categories: one, akin to arms control talks, in which the two countries' militaries discuss cyber-related dangers they pose to one another—figuring out how to avoid escalation due to a cyber incident—and another in which diplomats cooperatively look to address common cyber threats. Non-government experts' participation in building bridges between the two countries in the cyber realm could also prove fruitful, even in combatting threats that include a cyber component, such as terrorism and organized crime.

Moscow and Washington should reinvigorate and advance both multilateral and bilateral diplomatic efforts on cyber policy. This includes continuing work within the U.N. in both the OEWG and the GGE formats, not least of all because increased agreement on cybersecurity between Russia and the U.S. would get the world closer to global norms, rather than fragmenting it further into opposing coalitions. Likewise, it is worth thinking about restoring the bilateral confidence-building measures adopted in 2013, slowly working toward a formal agreement and making at least top-level declarations that would send a clear message to non-state actors that may be involved in hostile cyber activities.

Dialogue, in my view, should always be chosen over unilateral actions—including public allegations and sanctions—and, as difficult as it is, measures should be reciprocal. Here, I do not have a specific set of measures in mind but refer to the principle of parity that marked Cold War-era agreements. Needless to say, cyber relations are asymmetrical by their very nature and there is too much secrecy involved to make mirror-image policies possible. However, reciprocity, as opposed to unilateral measures, is key to bilateral agreement and some measure of it must be introduced into the equation somehow.

Conclusion: In Search of Understanding

By Natasha Yefimova-Trilling and Simon Saradzhyan

As this paper was being written, new headlines related to U.S.-Russian frictions in cyberspace grabbed our attention with regrettable regularity. The cycle of cyber action and reaction—with its breaches, ransomware, sanctions or other punitive measures—seems to never end. The persistence of this cycle throws into stark relief the fundamental challenge facing the Cold War-era foes: how to manage bilateral cyber contention in ways that keep the two nuclear superpowers from stumbling into war.

The authors of the paper's two halves share this concern. Despite all the differences in their vantage points, they agree that cyber-related risks in U.S.-Russian relations pose the threat of real-world harm to lives and property. They also agree that U.S.-Russian relations in the cyber domain are marked by mistrust and misperceptions that have become increasingly difficult to surmount. In some ways, this dynamic mirrors larger differences in the bilateral relationship, such as the countries' approaches to the tensions between national security and personal freedoms or the conviction in both capitals that the other side is bent on stirring up popular discontent and political upheaval on their home turf. But, due to ICTs' pervasiveness in everyday life, the cyber domain fills each country with new anxieties about vulnerability to cyber intrusions that do damage once thought possible only through kinetic warfare or hands-on sabotage—in governments, power grids, pipelines. It seems that progress toward improved U.S.-Russian relations in the cyber domain will require teams of thoughtfully, deliberately, perhaps creatively selected interlocutors—not just technical specialists, diplomats and other government officials, but possibly private-sector experts and specialists on negotiations as well. Clearly, the challenges now testing the bilateral relationship involve not just foreign policy, international security or ICTs per se but psychology and cultural differences as well.

These myriad challenges have led the paper's authors to conclude that a formal U.S.-Russian bilateral agreement on cyber rules of the road is not possible now or in the near future. However, they still believe there is pressing need for continued bilateral engagement, Track 2 or 1.5 expert dialogue and confidence-building measures. Both the Russian and U.S. authors point out that the two countries need a better understanding of each other's cyber postures, including red lines and other significant cyber-related policies, especially concerning retaliation but also including mundane-seeming details such as definitions of relevant terms. Without making progress in these areas the sides cannot make progress toward reducing the risk that a cyber incident could fuel escalation into a war that would be in neither's interest.

RM student associates Thomas Schaffner and Anastasiia Posnova and special projects editor Natasha Yefimova-Trilling contributed research to this paper.

The opinions expressed herein are solely those of the authors.

Appendix 1

11 Voluntary, Non-Binding Norms for Responsible Behavior of States in Cyberspace

Recommended in the 2015 U.N. GGE Report

(a) Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;

(b) In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences;

(c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;

(d) States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect;

(e) States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;

(f) A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;

(g) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;

(h) States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;

(i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;

(j) States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;

(k) States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

Appendix 2

Research Questions Posed to Authors

I. Do the U.S. and Russia see a need (is it in their vital national interest) to establish rules of the road in cyberspace?

II. If it is in the vital interest of the U.S. and Russia to establish such rules, then:

A. What would be the benefit of having rules of the road for the U.S. and Russia (and third countries/the international community) and how would they outweigh potential costs?

B. Should these rules be:

1. Formal/binding or informal?

2. Bilateral or multilateral?

a. If bilateral, then should they apply to the U.S.-Russian dyad, regulating activities related to incidents in the bilateral relationship only, or to third parties, regulating activities related to incidents that involve third countries but that impact the U.S.-Russian relationship?

b. If multilateral, then should it be a U.N. product, OSCE product or NATO-Russia product? Could the Tallinn Manual serve as one of the foundations for a draft product, forming the basis of understanding for cyber warfare and law of armed conflict?

3. What would be the key concepts and definitions in such rules (e.g., should the sides rely on the U.S.-Russian glossary of cyber terms as developed under the auspices of the EastWest Institute or start from scratch)? If EWI's product is not sufficient, then

can you define among other things what cyber conflict and cyber war mean in your respective countries?

III. Which of the following sectors of the cyber domain should these rules cover? (multiple answers possible)

A. Investigation, attribution and prosecution of materially driven cybercrimes (e.g., credit card theft) by non-state actors and/or state actors.

B. Investigation, attribution and prosecution of cyber activities by violent extremist groups (that use ICTs for coordination, communication, recruitment and execution of attacks).

C. Investigation, attribution and prosecution of espionage by non-state actors and/or state actors.

D. The most egregious and pernicious activities in cyberspace (e.g., destructive malware encoded to access and disrupt critical infrastructure like financial services, electoral processes, energy, water, oil/gas, manufacturing, nuclear, etc.).

E. Attribution and response to offensive actions by non-state actors and/or state actors meant to disrupt critical civilian and military infrastructure, including energy grid, electoral systems, command and control systems.

F. Commitments by state actors to refrain from A and/or B (probably not feasible) and/or D (particularly important)?

IV. Regardless of whether rules are established or not, should the U.S. and Russia pursue confidence-building measures, e.g., cyber dialogue, joint cyber exercises, establishment of points of contact, working groups and (more) hotlines? Should we have CBMs for cybercrime and cyber terrorism, but maybe not rules of the road *per se*?

Russia Matters
The Cyber Project
The U.S.-Russia Initiative to Prevent Nuclear Terrorism

Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.russiamatters.org
www.belfercenter.org/Cyber
www.belfercenter.org/USRIPNT

Printed in the United States of America