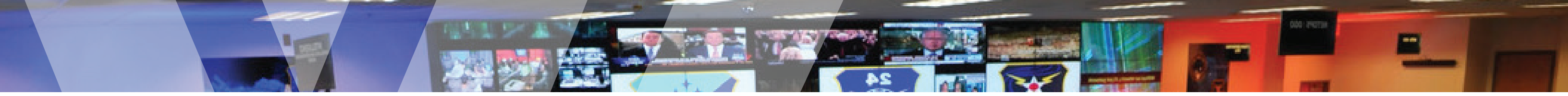

KENNAN CABLE

No. 41 I March 2019

Personnel with U.S. Cyber Command (Photo: US Air Force)

A Cyber Treaty with Russia

Robert G. Papp

Prospects for meaningful cyber negotiations with the Russian Federation, let alone a bilateral agreement or cyber treaty, seem almost impossible to imagine today. Our anguish over Russia's meddling in American elections, preoccupation with alleged ties between the Trump administration and the Russian government during the recently concluded Mueller investigation, and major disagreements on geopolitical issues including Ukraine, Syria, and Venezuela, have left us at an impasse. Instead of genuine dialogue between the United States and Russia, we see the two nations talking past each other and posturing to both domestic and international audiences.

More alarmingly, the very framework of bilateral and multilateral arms control treaties that got us through the last decades of the Cold War, starting in 1972 with the Anti-Ballistic Missile (ABM) Treaty and the interim Strategic Arms Limitation Agreement (SALT I), is in disarray. This process of unraveling likely began in 2002 when the U.S. withdrew from the ABM Treaty. The Russian Federation suspended its participation in the1992 Conventional Armed Forces in Europe Treaty in 2007 and completely halted its participation in 2015. Most recently, the U.S. announced, on February 22, 2019, its intent to withdraw from the Intermediate-Range Nuclear Forces (INF) Treaty signed in 1987.

Wilson Center

KENNAN INSTITUTE

Given these developments, proponents of treaties with Russia, whether bilateral or multilateral, now seem few and far between. Even the architects of past agreements must justifiably wonder what has become of their life's work. How, then, might negotiations leading to a cyber treaty be a viable policy option?

We may begin by asserting that treaties can and do have a shelf life. Technologies advance, military strategies change, and diplomatic positions and alliances shift, as do a nation's goals and priorities. Not every treaty has to last as long as the agreements forged in the Treaty of Westphalia (1648) or the Congress of Vienna (1814-15) to have a profound effect. Successful reduction of the risk of nuclear and conventional war over the last half-century has amply demonstrated the value of negotiating with the Soviet Union, and later the Russian Federation, even when treaties have ended over time in violations, recriminations, and withdrawals.

The Secret of Politics? Make a Good Treaty with Russia

To move forward with Russia today, we would do well to learn from the past. Germany's "iron chancellor," Otto Von Bismarck, declared in 1863: "The secret of politics? Make a good treaty with Russia." Caught between rivals Russia and France, Bismarck understood that an accommodation with Russia would give him the time and security to pursue his top goal, German unification. His negotiation of the Treaty of Berlin following the Russo-Turkish War of 1877-78, and the Reinsurance Treaty almost a decade later (a treaty that lasted only three years), was not popular with militarists at home who advocated a preemptive war with Russia. Yet Bismarck succeeded in unifying Germany, and Germany did not go to war with Russia until 1914.

> It is in our national interest to negotiate some limits to this activity to reduce these threats and the human and financial resources needed to address them.

Today, the U.S faces two main nation-state rivals in cyberspace, Russia and China. This rivalry unfolds in the context of multiple conventional challenges facing our over-extended military and security forces, including deployments in war zones, North Korea, Iran, terrorism, and regional conflicts. In the case of cyberspace, there is already an insatiable demand to recruit, train, and retain qualified personnel in both government and the private sector. We recognize the potential for massive harm that nation-state sponsored cyber-attacks present. It is in our national interest to negotiate some limits to this activity to reduce these threats and the human and financial resources needed to address them.

In contemplating a cyber treaty with Russia, traditional arms control negotiations give us ample lessons to draw from. Even if no longer in effect, the INF, CFE, and other strategic treaties had a full and valuable service life and achieved their purpose well. The elaborate verification and confidence-building measures made possible through arms control treaties provided us greatly enhanced security. They established protocols and venues for dialogue among genuine experts when things inevitably went awry. The CFE Joint Consultative Group is one such example: staffed by experts from the 22 signatory nations, the group was always ready to discuss the smallest perceived violation. The on-site inspections of the INF treaty supplemented national technical means, and, perhaps most importantly, fostered constant communication among U.S. and Russian counterparts.

We were genuinely concerned about the prospect of a full-scale conventional or nuclear war with Russia when we signed these treaties. Negotiating them was not a sign of weakness or capitulation, but rather one of strength. We continued to build and improve our military forces in ways that met our global national security objectives. Ronald Reagan came to see the value in arms control treaties, even as he started a massive investment in missile defense (the Strategic Defense Initiative). He certainly was not "soft" on the Soviet Union when he signed the INF Treaty and set the Strategic Arms Reduction Treaty negotiations on a path to its entry into force in 1994[1]. Decades later, most Americans no longer go to bed at night worrying about a massive attack on the homeland by Russia. While both nations retain considerable capabilities, nuclear fallout shelter drills are a distant memory. Today, some abandoned U.S. missile silos even serve as trendy subterranean residences.[2]

The Evolving Cyber Threat

Cyberspace has emerged as one of our overwhelming national security preoccupations, affecting the state, private sector, and individual alike. Hardly a news cycle goes by when we do not hear of some new hack by unknown or unverified actors or are ourselves one of millions that are directly affected. Commercial breaches have become so commonplace that we are now familiar with the well-worn response: an offer of a year of free credit monitoring, a weak public apology from the CEO, and a brief drop in the company's share price. Then we move on to the next event.

More unsettling, but hardly unpredictable, is the inexorable expansion of nation-state cyber operations into the centuries-old practices of covert influence. This has ranged from the manipulation of information and creation of "fake news," to theft and public exposure of sensitive data and intellectual property outside of pure military and intelligence targets, and interference in elections. Documented Russian cyber operations in Estonia, Ukraine, and Georgia have demonstrated just how damaging these attacks can be.[3] They also provide clear indications of what Russia identifies as its critical security interests, and its willingness to act on those interests.

Further, the target list of cyber-attacks attributed to sovereign states has expanded well beyond traditional espionage objectives to include institutions such as the World Anti-Doping Agency and the International Olympic Committee (by Russia), Sony Pictures (by North Korea), and the Office of Personnel Management (by China). What was once the domain of spies, agents of influence, physical theft, signal intercepts, media campaigns, and other covert techniques can now be accomplished remotely and inexpensively through the Internet.

We must understand that cyber-targets that are acceptable to one country may not be to another. The U.S. may argue that state-sponsored hacking to uncover and benefit from commercial secrets is out of bounds; the Chinese and Russians clearly have other views. Surely, we engage in activity they do

Speech at the plenary session of the International Cybersecurity Congress. July 6, 2018, Moscow.
Photo: Mikhail Metzel

not like, whether in the cyber arena or in other areas where we have distinct advantages.

Finally, there is a long and convoluted history contesting who did what first in the realm of cyber warfare. The Stuxnet cyberattack on the Iranian Natanz nuclear enrichment facility, first detected by the International Atomic Energy Agency in 2010, is one such case in which the United States stands accused of changing the rules on cyber activity.[4] The alleged repurposing of U.S. hacking tools by criminals and nation-states in such cases as WannaCry and NotPetya cloud lines of responsibility and accountability.[5]

The Need for a Cyber Treaty

In the current environment of accusations and counter-accusations, and the virtual absence of any meaningful dialogue between the U.S. and the Russian Federation, a period of genuine negotiations over cyber conduct would be of value.[6] The Russians and Chinese saw a clear need for such bilateral engagement when they cut a deal in 2015 not to conduct cyberattacks against each other that could "destabilize the internal political and socio-economic atmosphere," "disturb public order," or "interfere with the internal affairs of the state."[7] Both wanted to avoid the cyber version of the two-front war that so preoccupied Bismarck. They did not actually need a full-blown treaty to do this, as both knew that the cyber "front" they would be focused on was not each other.

The United States did negotiate with China to reign in cyber espionage during the Obama administration, in a limited effort that likely had at least some salutary effect on the level of Chinese commercial espionage. The agreement's fatal flaw, however, was in being vague and non-enforceable.[8] Such agreements can be effective when there is clear "good will," but an unambiguous treaty with implementation and verification mechanisms, especially when dealing with a clear adversary, would certainly be preferable. President Reagan's adaptation of the Russian proverb "trust, but verify" still resonates.

Even a cyber treaty of limited duration with Russia would be a significant step forward. While our current domestic political situation, and the very recent demise of the INF treaty, may not offer the best environment for negotiation, we should at least start laying the groundwork for negotiations. Within a few years, the world will have moved well beyond our current conceptions of cyber warfare to include broader applications in the realms of artificial intelligence, identity management and biometrics, DNA data manipulation, and technological advances of which we have not yet conceived.

Even today, there is no internationally recognized definition of what constitutes a cyber-attack, although the NATO-sponsored "Tallinn Manual" of 2013 did lay out some fundamentals. With its 2017 revisions, the "Tallinn Manual" provides a solid foundation for negotiating global norms and could serve as the basis for future "digital Geneva Conventions."[9] A multilateral approach to a cyber treaty, however, could take years to come to fruition, and would not address our immediate security concerns with the Russian Federation. Efforts such as the Paris Call for Trust and Security in Cyberspace, subscribed to by 64 nations and numerous corporations and organizations as of January 23, 2019, are noble but lack the enforcement mechanisms needed to ensure compliance.[10]

The stakes are high. Cyber reconnaissance of the U.S. electrical grid, energy sector, and nuclear power industry are obvious causes for concern. The assault on our digital economy and online lifestyle should be as well. Hacks of social media attributed to Russian state-sponsored actors, both real and imagined, are ubiquitous. Intrusions into platforms such as Facebook and Twitter have shaken our confidence in widespread means of communication that increasingly dominate our lives. The political divisions and infighting caused by Russian cyber intrusions are perhaps equally significant.

Matters will only worsen. Cyber options are a valuable tool for nation-states, both to achieve immediate policy goals and in "preparation of the battlefield" for future conflict. Assessing the source of an attack, especially when the attacker takes care to cover his tracks, is difficult. Attribution is even more complex in an era of trolls, proxies, patriotic hackers, ubiquitous encryption, increasingly sophisticated obfuscation techniques, and independent hackers simply seeking acclaim for their skills. Publicly revealing who gave the order, even when possible, inevitably involves the revelation of sensitive sources and methods that can be more damaging than the actual attack. Indictments and public shaming of cyber actors are increasingly valuable tools, but have done little to alter Russian cyber policies. In some cases, our responses may even benefit the attackers, either through providing feedback on our tactics, or resulting in recognition and reward back home.

A Cyber Treaty with Russia

Given these myriad challenges, what would a cyber treaty with Russia look like? We would need to start with terms of reference, carefully defined and mutually agreed upon. The "Tallinn Manual" could be a starting point, although the Russian Federation played no part in its drafting and would want its own input. Russia first proposed a cyber limitation resolution before the UN General Assembly in 2008, for example.[11] Ten years later, we now confront a dizzying array of areas vulnerable to cyberattack, including military, national security, commercial and industrial, political and electoral, and social media. Identifying and categorizing these clearly will be essential.

One would not expect for a moment that espionage against legitimate military and national security targets could or should end, nor preparations for cyberattacks against these in wartime. Negotiators will need to clearly elaborate exactly which targets would be prohibited, and under what circumstances. For example, while hacking military command and control systems likely would fall outside the scope of a treaty, attacks on air traffic control or theft of aerospace industry information could be prohibited. Addressing cyber intrusions into a civilian power grid connected to a nuclear or command and control center might provoke a more vigorous debate. One argument might be that Supervisory Control and Data Acquisition (SCADA) systems or Internet of Things (IoT) devices at the center might not be subject to limitations, but intrusions that could shut down a nearby hospital would be covered. Given the complexity of such targeting, many issues would have to be addressed, not necessarily with the goal of prohibiting them, but at least to establish a mechanism to address these threats when detected.

The most important element of treaty negotiations, however, would be how to handle perceived violations. There is little doubt that denial of responsibility, plausible or otherwise, would often be the first response of the accused party. Such denial has been true in treaty implementation throughout history, from the obvious massing of troops on a national border to the use of prohibited weapons systems. Active mechanisms to enable dialogue among genuine experts will be the key to success. Above all, the goal must be to avoid the rapid escalation of misunderstandings that could lead to reprisals or even armed conflict.

> One would not expect for a moment that espionage against legitimate military and national security targets could or should end...

A cyber treaty, with the establishment of formal deconfliction, verification, and inspection mechanisms, could take very clear cues from previous arms control treaties. While cyberattacks are very much based in the real and physical, from servers, routers, data storage facilities, and cloud infrastructure, to the very buildings where cyber operators work, we are not talking about counting tanks or inspecting missile production facilities. Rather, such measures as investigation of IP addresses, unpacking of malware by investigators, procuring records from internet service providers, identifying botnets, and other technical measures might be envisioned. Absolute specificity of intent and action will be required in any treaty language.

As we learned in arms control, Russians are pragmatic and not prone to acting "in the spirit" of an agreement. In the CFE treaty, for example, one variant of gun barrel destruction by explosive charges required that "the tube is split or longitudinally torn within 1.5 meters of the breach."[12] That is the kind of clear language that will be needed for effective compliance, and the Russians both understand and prefer lack of ambiguity. Revisions over time to keep pace with technological developments will be essential. Neither the Americans nor the Russians will be eager to reveal capabilities or vulnerabilities through the process of negotiating an agreement on cyber conduct. Cyber verification is not the same as counting missiles, and inspection and confidence-building visits to cyber and signals intelligence facilities are unlikely ever to be envisioned or even relevant. Consider, however, that not so long ago the INF Treaty allowed us to perform non-intrusive cargo scans of train cars and ski around the Votkinsk Machine Building Plant looking for holes big enough to exfiltrate an SS-20 missile. We arranged a mechanism to schedule and route flights over our respective territories under the multilateral Treaty on Open Skies. These seemed impossible before they happened. Perhaps the required leap in cybersecurity may not be as far as it seems.

Cyberspace Will Be about More Than Cyberspace

Technical negotiations will not go far unless we come to terms with the sources of recent Russian behavior, and what underpins its increasingly aggressive international posture. If the exact decision chain leading to Russia's increasing cyber intrusions abroad is not yet fully understood, the underlying rationale is comprehensible. Russia is acting on a litany of complaints about U.S. actions over time, including our development of SDI; NATO expansion; events in Ukraine, Georgia, and the Baltic states; deployment of anti-ballistic missile systems in Eastern Europe; and sanctions.

We do not need to accept their assessment that the United States acted, purposely or not, to humiliate Russia immediately after the fall of the Soviet Union. We also do not have to agree with Putin's thesis that we have interfered in its domestic politics and that of its former Soviet neighbors. We do need to accept that Russia believes this. We should understand that this resentment underlies, but does not justify, its use of cyber tools against institutions we believe to be off-limits. Russian actions reflect the country's willingness to use proven and highly effective means to counter U.S. influence, prestige, and political stability. Negotiations on the technical aspects of cyber conduct will not take place in a vacuum. Both sides have to address, even if not resolve, a variety of side issues if any negotiation is to take place, let alone succeed.

We may also find that the Russian government is less eager to enter into negotiations over cyber conduct than in 2008, given its own advances in information warfare. It has met with success in recent years, as widely cited in FBI and DHS reporting.[13] Yet Russia must know that the United States has tremendous capabilities of its own, and that the gloves may be coming off. A new emphasis on U.S. cyber offensive capabilities and the 2009 establishment and subsequent growth of Cyber Command, should clearly demonstrate this.

The Russians have much to lose in a cyber "gonka vooruzhenii," as the last "arms race" cost them dearly. Russia is under no illusion that we have a far greater reserve of resources to mobilize in this new arena as well.

In a comment to President Trump in July 2018, President Putin reportedly offered to conduct a joint investigation of the Main Intelligence Directorate (GRU) officials indicted by special counsel Robert Mueller for the 2016 Democratic National Committee hack. The American public and policymakers justifiably met this offer with derision and outrage. Accepting such an offer from the accused party in this case would have been unwise and even counterproductive.

Opening a discussion about setting boundaries for cyber activity going forward, however, need not be seen as weakness or folly. It is precisely when bilateral relations are plumbing new depths, and there seems to be no hope for improvement, that our professional national security establishments must engage. Domestic political considerations are currently the most daunting challenge for such negotiations—in both countries. Coming to the table to reduce the risks of further and potentially catastrophic cyber miscalculations must take precedence among policymakers on both sides that value our shared future. Starting on the path to a cyber treaty is an ambitious but not unthinkable goal.

Footnotes

[1] For a nuanced summary of these themes see Daryl G. Kimball, "Looking Back: The Nuclear Arms Control Legacy of Ronald Reagan," *Arms Control Today*, July 1, 2004 (online version).

[2] See underground-homes.com, silohome.com, and even Zillow.com for examples.

[3] For a concise timeline of these and other operations see Robert Windrem, "Timeline: Ten Years of Russian Cyber Attacks on Other Nations," nbcnews.com, December 18, 2016.

[4] For a detailed discussion of this issue see Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014).

[5] For a discussion of these tools, see "NotPetya and WannaCry Call for a Joint Response from International Community," NATO Cooperative Cyber Defence Centre of Excellence online post,June 30, 2017.

[6] For adiscussion of how little the two sides are engaging, the May 19, 2018 debate between historian Stephen Cohen and Ambassador McFaul at Columbia University is a comprehensive start. Wherever one falls in this debate, the common theme that substantive dialogue must be restored does resonate. A video of this debate sponsored by the Harriman Institute of Columbia University and New York University is available on YouTube.

[7] Olga Razumovskaya, "Russia and China Pledge Not to Hack Each Other," *Wall Street Journal,* May 8, 2015.

[8] For a discussion of this agreement see "U.S.-China Cyber Agreement," *CRS Insigh*t, October 16, 2015 (IN10376).

9. Tarah Wheeler, "In Cyberwar, There Are No Rules: Why the World Desperately Needs Digital Geneva Conventions," *Foreign Policy*, Fall 2018, 36-41.

10. "Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace," France Diplomatie website, diplomatie.gouv.fr.

11. TomGjelten, "Shadow Wars: Debating Cyber 'Disarmament'," *World Affairs*, November/December 2010, 3. The resolution passed 178-1 with the United States opposed. The article also outlines other Russian "information terrorism" resolutions dating to 1998, and the Shanghai Cooperation Organization accord of 2009.

12. *Treaty Between the Twenty Two Sovereign Nations on the Reduction of Their Conventional Armed Forces in Europe* (Washington, DC: On-Site Inspection Agency, November 19, 1990), Section V.23 (A).1.

13. Simon Shuster, "This KGB Chief Rang the Alarm About Russia-U.S. Cyberwar. No One Listened," *TIME*, March 25, 2018.

The opinions expressed in this article are those solely of the author.

Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue NW
Washington, DC 20004-3027

Robert G. Papp retired in 2017 after service as a naval officer and a career in federal civil service, including as director of the Center for Cyber Intelligence at the Central Intelligence Agency. He is a graduate of the U.S. Naval Academy and Georgetown University, and holds a PhD from Columbia University, where his dissertation focused on the late Imperial Russian stock market. He works as a consultant and speaker.

The Wilson Center

wilsoncenter.org
facebook.com/WoodrowWilsonCenter
@TheWilsonCenter
202.691.4000

The Kennan Institute

wilsoncenter.org/kennan
kennan@wilsoncenter.org
facebook.com/Kennan.Institute
@kennaninstitute
202.691.4100

Wilson Center

KENNAN INSTITUTE