Will Russia's Efforts to Prevent the Weaponization of Information Succeed?

Sharikov, Pavel

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Sharikov, P. (2020). Will Russia's Efforts to Prevent the Weaponization of Information Succeed? *Russian Analytical Digest*, 259, 12-14. https://doi.org/10.3929/ethz-b-000454007

ity goes a long way toward shaping decisions, but the military edge plays at best a marginal or insignificant role. Indeed, abstract perceptions of superiority or inferiority are largely irrelevant once it has been established that the opponent has the means to resist and that the fight may escalate.

There is no need for NATO or the United States to project the ability to win in the initial period of war, since victory is hardly a requirement of deterrence. The possibility of a sustained battle effectively eliminates the prospect of a fait accompli strategy. Warfighting, be it through annihilation or attrition, inherently carries risks and costs that are not likely to be commensurate with prospective Russian gains in the Baltics. This makes positional fait accomplis, gains in relative position that do not involve territorial revisionism, much more lucrative, especially for nuclear powers in a context where war carries the risk of nuclear escalation.

To be clear, there are reasons why Moscow and NATO might come to blows, but there is little evidence for the notion that Russia harbors a fait accompli strategy or has need of one. This article renders no judgment on whether Moscow has designs on territorial revisionism writ large, simply on the premises that govern U.S. and NATO defense planning and scenario constructs. The notion of NATO as object, or *casus belli*, has proven the most puzzling. Alliances are sabotaged or neutralized through subversion, steady erosion of relative influence, and wedging strategies (which generally fail), rather than objectless declarations of war. Hence, NATO remains safe from overt challenges, but vulnerable to death by a thousand cuts and the internal disconnect between its desire for greater cohesion along with a desire for further enlargement.

About the Author

Michael Kofman serves as Director of the Russia Studies Program at CNA and as a Fellow at the Kennan Institute of the Woodrow Wilson International Center in Washington, DC. His research focuses on Russia and the former Soviet Union, specializing in the Russian armed forces, military thought, capabilities, and strategy. Previously, he served as a Program Manager and subject matter expert at National Defense University, advising senior military and government officials on issues in Russia and Eurasia. Mr. Kofman is also a Senior Editor at War on the Rocks, where he regularly authors articles on strategy, the Russian military, Russian decision-making, and related foreign policy issues. Mr. Kofman has published numerous articles on the Russian armed forces and security issues in Russia/Eurasia, as well as analyses for the U.S. government.

ANALYSIS

Will Russia's Efforts to Prevent the Weaponization of Information Succeed?

Pavel Sharikov (Institute for USA and Canada Studies, Russian Academy of Sciences, Moscow)

DOI: 10.3929/ethz-b-000454007

Abstract

In September, Russia made another effort to negotiate the nonmilitary use of cyberspace with the United States. Predictably, Washington rejected the proposal, despite admitting the urgency of the issue and the need to find a consensus solution with Moscow. The problem is not new: Russia has insisted on establishing common cyber norms in the United Nations for a long time, while the US has reserved the right to develop its own military cyber capabilities and blocked all Russian initiatives. With the stakes raised dramatically, Russia and the US have to find a way to agree on cybersecurity.

Russia's Proposal to the US

President Putin suggested a comprehensive information security program to the US. It was predictable that the US would reject the Russian proposal, for many reasons. First, an agreement with Russia on any issue, especially on cybersecurity, is political suicide for Donald Trump. Second, regardless of Donald Trump's relations with Vladimir Putin, the American political establishment would never believe that Russia is not interfering in the elections: Russia's voluntary commitment not to meddle

with the elections is not credible in the US. Third, Russia expects the US to cease what the Russian authorities see as American interference in Russia's domestic politics, primarily the free press and critical reports about the Russian government. The US sees this as a violation of freedom of speech.

The Russian proposal is the continuation of a two-decade-long crusade to prevent the militarization of the Internet. The history of Russia's efforts can be divided into three major periods, reflecting Russian domestic policies as well as changes in the international environment.

Three Periods of Information Policy

Between the late 1990s and the mid-2000s, the Internet was chaotic. The US established the Internet Corporation on Assigning Names and Numbers (ICANN), an organization that was seen in Russia as an attempt to dominate cyberspace. Russia introduced a UN resolution that called for information technologies not to be used for non-peaceful purposes. Since that time, Russia has led the international drive for Internet governance, including making a significant contribution to the establishment of a vehicle for this debate at the UN: a Group of Government Experts (GGE).

Between the late 2000s and 2014, the Internet became more organized, mostly due to the activities of Internet giants. The Russian government was very concerned that social networks and social media were used for political means. The experience of the color revolutions and the Arab spring forced Russia to enhance government control over the Internet. The Russian and American positions grew a little closer. Russia still sought to regulate the Internet as a domain, but also reached a number of bilateral agreements (including one with the US) and regional accords.

Since 2014, we have seen a new stand-off between Russia and the West. It was predictable that Russia would want to build up its defenses against Western influence, which was seen in Russia as a deliberate information operation. The Russian government has adopted many measures to control Internet users, measures known collectively as the "sovereignization of the Internet," which is seen as an analogue of the Cold War-era Iron Curtain. Sovereign Internet is intended to ensure not only that the Russian people only have access to the proper information, but also that international audiences receive information that the Russian government considers "reliable." Thus, the foreign policy dimension of sovereign Internet is as important as the domestic aspect. Russia still rejects the military use of the Internet and has succeeded in bringing together an international coalition around the idea of countering the weaponization of information.

2018 became a significant landmark in Russia's Internet governance crusade. The UN adopted two resolutions, one sponsored by Russia and its allies and the other introduced by the U.S. and Western democracies. The Russian resolution included 13 norms of responsible behavior of states in cyberspace, as well as establishing a new vehicle for further discussions of Internet governance: the Open Ended Working Group. The American resolution prolonged the mandate of GGE. The two organizations have different tasks and do not compete, but rather complement each other. It is obvious that the establishment of global norms of responsible behavior in cyberspace is impossible without consensus between Russia and the US.

Cyber Security

One of Russia's key points is denial of the existence of cyberweapons. According to Russian decision makers, if cyberweapons are legally prohibited, no country would have legal authority to use the right of self-defense against a cyberattack. Instead, the Russian government suggests considering all forms of cyber aggression as crimes and treating them as such, developing tracks for cooperation in investigation and prosecution. Needless to say, many countries—chief among them the US—have developed robust military cyber capabilities.

While it is clear why military cybertechnologies are kept secret, it is also noticeable that even cybersecurity strategies are classified. The US has declared many times that Russia is among America's most serious cyber opponents.

American cybersecurity strategy declares that these opponents are constantly attacking U.S. cyber infrastructure. The document "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command" introduces the term "persistent engagement"—a continuous operation "below the threshold of armed conflict." "Persistent engagement" as described in the Strategy implies that opponents inflict some damage, but not sufficient damage to provoke U.S. retaliation through military operations.

Russia's denial of cyberweapons implies that other countries' open development of military cyber capabilities is most likely perceived as a declaration of hostile intentions and consequently a source of potential conflict. It is unclear how Russia would retaliate against cyberattacks. Arguments that Russia is not developing its own military cyber capabilities are not credible, especially in the US, which has leveled many accusations of cyber aggression. I believe it came as a great surprise to Russian diplomats that the issue of International Information Security was linked to accusations of election interference. Before those accusations, the U.S. argument against Russia's really peaceful proposals seemed weaker, but now that Russia has established a clear image as a "cyber aggressor," American criticism sounds much more solid.

After almost a month of silence, Washington finally answered Moscow's proposals after indicting 6 Russians—alleged GRU officers—on different charges of hacking. Secretary of State Mike Pompeo said, "These cyber activities demonstrate a complete disregard for public safety and international stability. Russia, which presents itself as a champion of stability in cyberspace, is in fact one of the global Internet's greatest disruptors. We call on Russia to put an end to its irresponsible behavior."

Assistant Attorney General for National Security John Demers added, "This indictment lays bare Russia's use of its cyber capabilities to destabilize and interfere with the domestic political and economic systems of other countries, thus providing a cold reminder of why its proposal is nothing more than dishonest rhetoric and cynical and cheap propaganda."

Trump's Weakness in Dealing with Russia

For many reasons, including domestic political factors, President Trump and his administration are clearly in no position to discuss cybersecurity relations with Russia. However, it is obvious that cybersecurity issues cannot be solved without dialogue between Moscow and Washington.

The US would likely be willing to discuss cyber security issues with Russia as part of arms control. But this would require a principal change in Russia's position: the acknowledgement that cyber is a weapon. President Trump's position on arms control has also been quite unclear. During John Bolton's time at the National Security Council, it seemed that the US was going to withdraw from every arms control agreement that somehow limited the development of American military power.

Democrats would likely be more willing to negotiate on arms control, including cybersecurity issues. But the Democrats can hardly agree to a noninterference agreement with Russia. First, it is impossible to agree on the subject of the agreement: cyber capabilities are impossible to count. Second, it is impossible to verify any commitment to an agreement on cybersecurity and ensure compliance.

If the Democratic Party takes the White House and increases its influence in Congress after the November elections, it is possible that Russian-American relations will become a little more pragmatic and a little less ideologically spoiled.

Russia's Position

Russia's proposal is difficult to take seriously; however, it should be noted that Moscow is ready and willing to negotiate and cooperate. A number of small steps seem feasible for Russia and the US in the field of cybersecurity.

First, the top Russian and American politicians could make a declaratory statement that they would refrain from cyber and/or information attacks against each other.

Second, assuming that military cyber capabilities would make it possible to inflict serious damage, it is important to cooperate on countering, prosecuting, and investigating cybercrimes and nonmilitary cyberattacks. It is clearly necessary to develop a glossary in order to ensure that diplomats speak the same language.

It is also obvious that no cybersecurity agreement between Russia and the US is possible without the general improvement of bilateral relations. Russia and the US have a lot of contradictions, which creates a situation where incidental escalation may lead to catastrophic consequences. Even if an incident happens in cyberspace, the escalation of the conflict can hardly be separated from physical space and the use of kinetic weapons. Confidence-building measures should not be in isolation from other issues that may cause conflict.

About the Author

Pavel Sharikov, PhD., is a senior research fellow at the Institute for USA and Canada Studies at the Russian Academy of Sciences, where he has worked since 2002, studying the American political system, cybersecurity policies, and Russian-American relations. He has participated in a number of exchange programs with the United States: in 2005 with the Center for International Security Studies at the University of Maryland and in 2008 with the George Washington University. In 2009, he defended a dissertation devoted to American cybersecurity policies. Starting in 2015, he taught a number of courses as an associate professor at Moscow State University. Most recently, he was a visiting research scholar at the Center for International and Security Studies at the University of Maryland, where he investigated Moscow's and Washington's mutual accusations of interference in elections and domestic affairs.

Further Reading

Sharikov, Pavel. "Alternative Approaches to Information-Age Dilemmas Drive US and Russian Arguments about Interference in Domestic Political Affairs." (2020). Available at: https://cissm.umd.edu/research-impact/publications/alternative-approaches-information-age-dilemmas-drive-us-and-russian.