# American Influence on Russian Information Warfare

https://www.e-ir.info/2020/09/24/american-influence-on-russian-information-warfare/

BRYAN NAKAYAMA, SEP 24 2020

Imagine a powerful country that is interested in influencing the domestic politics of other states using information technology. Since the 1990s, this country has leveraged information technology to secretly and not-so-secretly influence the availability of information in other countries to achieve its foreign policy goals. This country even went so far as to create a fake social media service to gather data on and study the population of a long-term foe with the intent of provoking social upheaval. In response to these activities, its former chief rival declared that this powerful country was conducting information warfare and that the rival needed to rethink their strategy to account for this new way of conflict. If you are an American you will likely guess that the countries in this sketch are Russia, Ukraine, and the United States. What if I told you that the powerful country was the United States, the long-term foe was Cuba, and the former rival was Russia in the 2000s/early 2010s?

The revelation of Russian information operations against the 2016 presidential election has been viewed by some as an unprecedented act; a revelation which suggested that the United States had been playing cyberwar checkers while Russia was playing information war chess. Scholars studying the evolution of Russian cyber-enabled information operations generally argue that they are the legacy of Soviet strategic thinking and propaganda practices. However, these debates have consistently overlooked actions taken by the United States during the 2000s and early 2010s which resemble contemporary information operations and were perceived by Russia as acts of information warfare that necessitated a response. This is not to engage in whataboutery, rather, I contend that reckoning with the American influence on Russia's perception of information warfare provides useful lessons for how we should think about the ambiguities of perception that impact information conflict. Additionally, it suggests that attempts to democratize states by influencing their information ecosystems will backfire. In the following, I'll first provide an overview of American information operations, then describe the Russian perception of these activities, and I will conclude by describing what lessons we can draw from this episode.

United States' foreign and domestic policy has for a long time viewed individual's access to information as a buttress of and necessary condition for democracy. Following on from this belief, U.S. foreign policymakers during the 2000s–2010s conducted aggressive democracy promotion programs using information technology that if conducted today by another country would be viewed as cyber-enabled information operations. These programs were inspired by a belief that the Internet and other information technologies were a "liberation technology" – that digital information flows enabled political organizing, expression, and provided avenues for government transparency facilitated democratization. In other words, United States foreign policymakers believed that information technology could enable democratic movements to succeed in overthrowing authoritarian regimes.

While these democracy promotion programs sound good in theory, they also violate the information sovereignty of those targeted states. Beliefs about the democratizing potential of information technology that contrast authoritarian censorship with democratic openness fail to recognize that all states, regardless of regime type, seek to exercise information sovereignty by managing the distribution of information within their borders. For example, the United Kingdom and the United States worked to have content produced by Daesh removed from the Internet. At the same time, violating the information sovereignty of rivals during peacetime and wartime is an element of inter-state competition. During the Cold War, the CIA funded Radio Free Europe/Radio Free Liberty to broadcast into the Soviet Union and Eastern Europe.

Far from unnatural, attempts to defend or violate information sovereignty are a feature of interstate competition – the desire to maintain information sovereignty underlined the accusation by the United States that Russia attempted to manipulate U.S. social media discussions by promoting fake news and conspiracy theories. Therefore, while digital democracy promotion has a laudable goal, the fact that it is premised on violating the information sovereignty of targeted states means that it will be perceived as a threat.

While the United States has funded programs to circumvent Internet censorship since the early 2000s, the scale and scope of these programs accelerated in the late 2000s as protest movements in Iran, Philippines, and Moldova utilized SMS and social media services like Twitter. Inspired by these protests, the U.S. Agency for International Development (USAID) used a stolen Cuban telecom database to create a fake social media service called ZunZuneo. Operating mainly over SMS and without Cuban government authorization, ZunZuneo would send its thousands of Cuban subscribers general interest content such as sports, weather, comedy, and mild political commentary in addition to allowing peer to peer messaging. After building up a subscriber base, USAID planned to use Zunzuneo to foment "smart mobs" whose protests would snowball into a broader democratic revolution. To do this, ZunZuneo built political profiles of their subscribers and planned to leverage this information to provoke protests. ZunZuneo shutdown when the USAID grant expired in 2012, the role of USAID in ZunZuneo was unknown until a 2014 Associated Press report. Interest in leveraging social media also extended to U.S. Central Command, which in 2011 contracted out the creation of a 'persona management system" which would allow service members to manage sock puppet accounts on blogs and social media to shape the narrative against ISIS.

Outside of social media, the United States conducted a variety of digital democracy promotion programs which undermined the information sovereignty of targeted states by helping their citizens circumvent content filtering and other Internet restrictions. These activities included training activists on how to use filtering circumvention software, political organizing through the Internet, and providing software and hardware for activists to manage their networks. The United States even took a direct approach to content delivery when the Voice of America dynamically altered news articles, including their web addresses, in order to circumvent content filters imposed by states. One of the key pieces of software funded and distributed by the United States was TOR—a program that anonymizes and allows users to bypass content filtering. While not the cause of the 2010 Arab Spring, these digital democracy promotion programs are viewed as having facilitated the growth and spread of these protests. One Arab Spring activist reflecting on the power of TOR stated.

there would be no access to Twitter or Facebook in some of these places if you didn't have Tor. All of the sudden, you had all these dissidents exploding under their noses, and then down the road you had a revolution…Tor rendered the government's efforts completely futile.

Therefore, these democracy promotion programs, by enabling certain flows of information, were viewed as potentially powerful tools for democratic revolution.

While these U.S. democracy promotion programs were not focused on spreading misinformation like contemporary Russian information operations, they were clear violations of the information sovereignty of other states. Some of these efforts, like ZunZuneo, seem to directly foreshadow contemporary concerns that Russia has used social media to organize protests within the United States. Therefore, policymakers and commentators need to be more appreciative of how the United States engages in actions that could be perceived as information warfare under the guise of democracy promotion. To appreciate this point it is worthwhile considering what Americans' reaction would be if Russia paid for activists to be trained in the United States on how to create misinformation, funded and promoted a program like a TOR which enabled users to escape government scrutiny and created a fake social media network to provoke protests. Of course, Russia was paying attention to the information conflict implications of these digital democracy programs…

Russian political and military leaders viewed the Eastern European "color revolutions," Arab Spring, and Libyan intervention as demonstrating a new way of conflict practiced by the West which involved political destabilization through non-military means. The role of social media and the Internet in these revolutions did not escape Russian notice and information technologies were viewed as a key vector of Western subversion. For example, in 2011 the

head of the Russian Academy of Military Sciences General Makhmut Gareyev wrote that

internet networks were implanted in Egypt, Tunisia, and Libya over a two-year period…At the right moment, a centralized order was issued across all networks for people to take to the streets." Similarly, then-president Dmitry Medvedev stated "look at the situation that has unfolded in the Middle East and the Arab world. It is extremely bad…This is the kind of scenario that they were preparing for us, and now they will be trying even harder to bring it about.

These events were a major point of analysis in the infamous article by the Russian Chief of General Staff Valery Gerasimov which explored how Russia should respond to this new way of conflict and gave birth to debates over "hybrid war." Altogether, Russian strategic thought viewed the American digital democracy promotion efforts as a new non-military information capability for regime change.

While there is no evidence to evaluate whether Russia directly chose to emulate American activities, it is clear that the confluence between American actions to undermine information sovereignty and these revolutions convinced Russia that they were in a strategic environment which placed a premium on information capabilities and information security. On the domestic side, Russia began constructing a large-scale Internet content filtering and censorship regime in 2012 where none existed before. Externally, the Russian annexation of Crimea seemed to follow the playbook laid out in Gerasimov's article and Russian strategy statements have come to echo the concerns and vision of conflict that emerged out of Russian analysis of the Arab Spring and color revolutions. The overall Russian emphasis on information warfare as a threat and opportunity was deeply influenced by American digital democracy promotion and ironically came as a surprise to many Americans in 2016.

The political scientist Arnold Wolfers distinguishes between two types of national security. First, "objective security" which is whether there are actual threats to national values. Second, "subjective security" which is whether a state fears a threat to national values. For Wolfers, this gap means that states react to threats differently on the basis of their perception. In the instance of information conflict, what for the United States may seem like democracy promotion is interpreted by Russia as a security threat that demands a response. For Russia, information manipulation may seem par for the course as a matter of international competition but to the United States, it is a radically new threat. This is because Russia placed a higher priority on information sovereignty in a world dominated by American social media, whereas the United States did not anticipate information threats because policymakers believed the internet could only reinforce democracy. Ironically, this threat is driving the United States to adopt many of those practices that it once derided.

What this means is that scholars, observers, and policymakers need to take seriously that their perceptions of activities in the information and cyberspace domains may not match those of their opponents. Scholars have acknowledged the ambiguity of interpreting cyber and information operations as signals between states, and these instances of American information operations demonstrate that this ambiguity needs to be recognized by policymakers who advocate violating other states' information sovereignty even for the most noble of ends. The United States and Russia both responded to what they view as novel threats – generating a pattern of strategic interaction wherein U.S. policymakers don't appreciate their effects on Russian threat perception and commentators overlook interactive dynamics. All in all, American digital democracy promotion must be understood as yet another chapter in the rising prominence of information operations in global competition.

---

## About the author:

**Bryan Nakayama** is a Visiting Lecturer in International Relations at Mount Holyoke College. His research takes a critical constructivist approach to understanding military innovation and how militaries understand space of conflict. He is currently preparing a book manuscript on the history and evolution of domains of warfare – air, space, cyberspace – as major elements of the United States security imaginary.