Will Russian Exploitation of Open Press Destroy U.S. Democracy?

by Nicholas Kane

> ***A democracy is only as resilient as its people. An informed and engaged citizenry is the fundamental requirement for a free and resilient nation. For generations, our society has protected free press, free speech, and free thought.[1]***
>
> ***— U.S. National Security Strategy, December 2017***

The 2017 United States National Security Strategy states that Russia is using information activities to undermine democracies.[2] During the 2016 U.S. presidential election, Russian-sponsored entities leveraged fake social media accounts to create and disseminate false information content to U.S. audiences via traditional and social media and amplified that content through bots, trolls, and Russian overt news outlets. Russia, like other adversary states, controls its domestic media, thereby controlling the internal and external narratives; whereas, the United States' founding principles of freedom of speech and freedom of the press do not permit control of the media by the government. This paper recommends a whole-of-society approach to build a resilient population without compromising these freedoms along two lines of effort: protection and prevention. American democratic freedoms present a potential vulnerability in a future conflict and an ethical dilemma for the United States.

The dilemma: can the United States continue to exist with its current principles of freedom of speech and press as the dynamics of interstate competition and conflict change in the Information Age? Is it consequentialist to compromise the freedoms of speech and press to ensure the American way of life can endure or does the U.S. maintain its principles and risk defeat and decline of American global power? If there is a compromise of any kind, the United States risks becoming the epitome of hypocrisy in the process and will lose legitimacy of its global narrative about democracy and the freedoms Americans enjoy. Such a compromise is unlikely, but Americans must dialogue on

Major Nicholas Kane is a U.S. Army officer currently serving as a student at the School of Advanced Military Studies at Fort Leavenworth, Kansas. He holds a Master of Military Arts and Science degree from the U.S. Army Command and General Staff College and a Bachelor of Arts degree in International Relations from Lehigh University.

creative ways to meet threats in the information environment while preserving legitimacy. Key questions include, "[w]hat domestic security measures are tolerable in a democracy? What rules should govern the collection of domestic intelligence, especially in light of new technologies that equip authorities with unprecedented capabilities for surveillance?"[3]

In the geopolitical climate, states compete with soft power in the information environment rather than engaging in declared armed conflict against a more capable military.

Globalization and advancements in technology brought about the dawn of the Information Age, arguably the latest military revolution, which recast society and the military in the late-20th and early-21st centuries. In this revolution, the weaponization of information and activities in the information environment shape conditions before armed conflict. In the geopolitical climate, states compete with soft power in the information environment rather than engaging in declared armed conflict against a more capable military.

Russia's New Generation Warfare (NGW) exemplifies this approach to conflict by employing soft, or informational, power to set conditions for achieving political objectives using all the instruments of national power in an integrated and synchronized manner. Russia employs these instruments in ways that do not cross thresholds that would lead to overt armed conflict with the West. This employment of soft power for deceptive or coercive purposes is called sharp power and typifies Russian NGW. Gideon Rose, editor for *Foreign Affairs*, proffers that, "…enemies of democracy are less violent and aggressive than their fascist predecessors, so war is unlikely."[4]

What Rose does not address is that the paradigm of war may have shifted to that of information and political warfare for Russia to exploit rather than face the United States' military advantage. Therefore, the United States must adapt to address asymmetric threats in the information environment.

Political warfare is but one aspect of an NGW strategy and is rooted in deception.

Three concepts are significant to modern Russian political warfare: reflexive control, maskirovka, and active measures. Reflexive control, defined by Russian information warfare expert Timothy Thomas is "…a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action."[5] Maskirovka is deception activity designed to mask or disguise the activity.[6] In this case, maskirovka obfuscates the identity and sponsor of content creators and disseminators with false personae. Finally, active measures is a Soviet-era term used to describe information, psychological, or political means conducted to advance Russian foreign policy goals and extend influence throughout the world.[7]

A RAND study published in 2018, outlines Russian means of employment for active measures via traditional and social media. The study codifies a three-step process that begins with the generation of false or misleading original content by Russian-affiliated media, or from data provided by hackers. Next, bots and trolls disseminate the content as mis-attributed personae and amplify content that resonates with target audiences. Finally, unwitting entities like media outlets, bloggers, and users lured in by clickbait, propagate the content to targeted audiences.[8] As U.S. news outlets and social media platforms attempt to identify and purge their comment sections and information ecosystems of foreign malign users, they run the risk of crossing the threshold of censorship. Legitimate

Russia	USA
New Type War	New Generation Warfare / Hybrid War (U.S. term); No parallel U.S. term for equivalent activity
Reflexive Control	Perception Management / Military Deception
Maskirovka	Tactical Deception
Active Measures	Covert Action

Table 1. Comparison of Russian and U.S. terminology.

users exercising their first amendment right of freedom of speech found themselves temporarily blocked by Twitter during a bot purge as a reaction to reports of Russian interference with the elections via social media.[9]

The Russian methodology of information warfare falls into two categories of activity, information technology and information psychology. During the 2016 United States' presidential election, Russian hackers penetrated the Democratic National Convention to collect data, which is an example of leveraging information technology - cyberspace operations in this case. Once Russian-associated hackers exfiltrated data from the servers, actors weaponized the information content and covertly disseminated damaging or false content to U.S. audiences. This creation and dissemination of content is an example of information psychology.

Russia and other adversaries are exploiting Western societies' open presses and preventing Western ability to influence their populations due to securitized media apparatus and information blockades, as in North Korea. Many news outlets are now linked to various social media platforms. This linkage creates additional vulnerabilities as false or misleading reports are more widely disseminated and the personal data that social media platforms collect can fall into malicious hands as seen with the Cambridge Analytica scandal for Facebook. Prior to the exposure of Russian interference in the election, users freely divulged their information to use various services, unaware that such data could be used to inform content generation by Russian actors that would have more impactful effects during the election. Content generated by the Internet Research Agency, a known Russian troll factory, reached up to 126 million Americans.[10] The global reach of the internet drives the need for a sense of urgency to counter Russian activities in the information environment through the development of a more resilient population.

To understand why Russian active measures via social media were effective in the 2016 U.S. election, one must know the scope of which information on social media influences the U.S. population. Two-thirds of Americans get at least some of their news from social media platforms, a key target for Russian information warfare.[11] The Pew Research Center conducted a survey that showed two-thirds of Americans consume at least some of their news from social media. Within that 67 percent, older, non-Caucasian, lower educated populations increased their consumption of news via social media.[12] Additionally, approximately 77 percent of Americans own a smartphone and a nearly three-

quarters own a desktop or laptop computer.[13] Therefore, American audiences have more access to information, and are more susceptible to Russian information psychological activities employed to manipulate audiences.

In the Information Age, the Western democracies must address problems with a whole-of-government approach, if not a whole-of-society approach. The United States must counter current Russian efforts in the information environment and build long-term resilience to disinformation campaigns that may destabilize Western democracies. Rose does acknowledge that one of the ways in which democracies can persist is to accept and adapt to the "information revolution."[14]

A whole-of-society approach is necessary to mitigate Russian threats to democracy in the information environment while maintaining faith in western democratic values.

A whole-of-society approach is necessary to mitigate Russian threats to democracy in the information environment while maintaining faith in western democratic values. Fundamental to any approach is education and awareness by the American public. By education, the author means media literacy, the ability to critically think and analyze viewed content, to conduct independent research and fact-checking, and to behave responsibly online and on social media. One of the conclusions from National Security Council-68 for dealing with the Union of Soviet Socialist Republics was: "Keep the U.S. public fully informed and cognizant of the threats to our national security so that it will be prepared to support the measures which we must accordingly adopt."[15] This 68-year old statement can still apply to the current domestic approach.

Protection and prevention are two significant lines of effort to ultimately achieve the same end: a U.S. population that is resilient against adversary misinformation campaigns to undermine the legitimacy of democratic values. As a means to achieve this end, the U.S. can establish a Joint Interagency Task Force focused on Russia and its malign behavior. Representatives from the Departments of Defense, State, Treasury, Justice, Homeland Security, and the Intelligence Community would comprise the core of this Joint Interagency Task Force.

For near-term protection activities, the Department of Homeland Security and Department of Justice would be key players in identifying both foreign and domestic threats and prosecuting those within their jurisdiction. Additionally, the Intelligence Community would also contribute to the detection and characterization of foreign threats. Those foreign threats such as state-sponsored criminal entities or governmental entities create and disseminate content to foment discord in the United States. These entities also undermine the legitimacy of Western democracy, but the previous departments, through the detection of threats, can cue the Departments of State, Defense, and Treasury to pursue unilateral action to arrest or mitigate malign Russian influence, or seek assistance from the international community of interest.

For long-term prevention activities, elements of the Joint Interagency Task Force, the Department of Education, and the traditional and social media platforms can contribute to achieving the strategic end as well. Cooperation of these entities can lead to a nation-wide program of education focused on media literacy and online identity management, a more responsible effort to inform the population with objective news, rather than politically-leaning news, and social media companies that take greater responsibility in preventing malign influence while still maintaining users' freedom of speech. These are ways the United States can

develop a more resilient information enterprise and American population that supports and maintains democratic values.

Another potential prevention activity is governmental agency cooperation with the commercial enterprise to innovate new technologies that can project free internet into denied areas so truthful information can reach informationally repressed populations. This countermeasure could serve as part of a long-term strategy to inform regional audiences and provide alternative narratives to their own domestic state-run propaganda. These technologies would serve as a way to circumvent Russian suppression techniques of blocking certain websites or targeting specific end users Russia deems dangerous.

Internationally, the United States Government should continue efforts to promote internet freedom programs and facilitate growing access to free information, especially in authoritarian states. Additionally, Canada's Minister of Foreign Affairs Chrystia Freeland stated at a G7 summit on 23 April 2018, "[c]oordinated; action and cooperation are needed to build resilience and reinforce our democratic institutions and process against foreign interference by state and non-state actors,… [t]here are consequences for those who seek to undermine our democracies."[16] These remarks addressed Russian malign behavior toward Western democracies, indicating a unity of effort against Russia to curb demonstrated behaviors. The United States must remain actively involved in this unified front against Russian malign behavior.

In future competition and conflicts, the information instrument of power and leverage of information-related capabilities such as cyberspace operations or inform and influence activities, will have a significantly greater role through the spectrum of conflict. Successful states will employ a whole-of-nation approach more effectively than their adversaries by synchronizing the instruments of national power, leveraging the commercial sector, and mobilizing an informed population, especially in the competition space before declared conflict. Russia demonstrated its willingness to execute active measures and propaganda to undermine faith in democracy and foment discord amongst populations of Western democracies. Without U.S. and friendly state action, Russia will continue to behave maliciously in its national interests.

George Kennan posited that "[t]o avoid destruction the United States need only measure up to its own best traditions and prove itself worthy of preservation as a great nation."[17]

In the Information Age, one must question whether this idealistic statement made in 1946 is still valid? Seventy-two years later, Joseph Nye echoes Kennan's sentiment stating, "…democratic government and societies should avoid any temptation to imitate the methods of their adversaries," about addressing Russian information warfare.[18]

The United States can apply elements of its strategy towards Russia from the beginning of the Cold War, however, advanced technology and the internet mitigated the protection of geography the United States once enjoyed. The United States must adapt to the modern environment, but above all, the nation must remain steadfast in its adherence to American values and freedoms. ***IAJ***

NOTES

1 Office of the President of the United States, *The National Security Strategy of the United States of America*. (Washington, D.C.: U.S. Government, 2017). 14.

2 Ibid.

3 Amichay Ayalon and Brian Michael Jenkins, "War by What Means, According to Whose Rules? The Challenge for Democracies Facing Asymmetric Conflicts: Proceedings of a RAND-Israel Democracy Institute Workshop, December 3-4, 2014," (Santa Monica: RAND Corporation. 2014), 1.

4 Gideon Rose, "Is Democracy Dying?" *Foreign Affairs*, (May/June 2018), 8.

5 Timothy Thomas, "Russia's Reflexive Control Theory and the Military." *Journal of Slavic Military Studies* 17 (2004): 237-256. (Oxford: Taylor & Francis Group), 237. DOI:10.1080/13518040490450529

6 Timothy Thomas, *Recasting the Red Star*, (Fort Leavenworth, KS: Foreign Military Studies Office, 2011), 384.

7 Scott Marler, "Russian Weaponization of Information and Influence in the Baltic States" (MMAS Thesis, Command and General Staff College, Fort Leavenworth, KS, 2017), 69.

8 Todd C. Helmus, et al., *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*. (Santa Monica: RAND Corporation, 2018), 12.

9 BBC News, "Twitter Bot Purge Prompts Backlash," *BBC News*, 21 February, 2018, accessed 24 April, 2018. http://www.bbc.com/news/technology-43144717.

10 Amol Rajan, "Can Democracy Survive Facebook?" *BBC News*, 1 November, 2017, accessed 23 April, 2018. www.bbc.com/news/entertainment-arts-41833486.

11 Elisa Shearer and Jeffrey Gottfried, "News Use Across Social Media Platforms 2017," *Pew Research Center: Journalism & Media*, 7 September 2017, accessed 23 April, 2018. http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017.

12 Ibid.

13 Pew Research Center: Internet and Technology Fact Sheet, *Pew Research Center*, 5 February, 2018, accessed 23 April, 2018, http://www.pewinternet.org/fact-sheet/mobile.

14 Rose, 8.

15 The Executive Secretary to the National Security Council, "A Report to the National Security Council by the Executive Security on United States Objectives and Programs for National Security" (NSC-68), 15 April, 1950, 63.

16 David Ljunggren and Lesley Wroughton, "G7 Foreign Ministers Condemn Russian Behavior, Says it Impedes Cooperation," 23 April, 2018, accessed 24 April, 2018. https://www.reuters.com/article/us-g7-summit-foreign/g7-foreign-ministers-condemn-russian-behavior-says-it-impedes-cooperation-idUSKBN1HU1OS.

17 George F. Kennan, "The Sources of Soviet Conduct," *Foreign Affairs*, (1947): 566-582, 582.

18 Joseph S. Nye Jr., "How Sharp Power Threatens Soft Power: The Right and Wrong Ways to Respond to Authoritarian Influence," *Foreign Affairs*. 24 January, 2018, accessed 22 April, 2018. https://www.foreignaffairs.com/articles/china/2018-01-24/how-sharp-power-threatens-soft-power.