REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 23 May 2018	**2. REPORT TYPE** Final	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE

The U.S. Needs Trolls: Strategic Concepts to Command the Gray Zone Struggle Technology and Doctrine to Revolutionize Influence Warfare

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Joshua S. Samet, U.S. Department of State

Paper Advisor: Dr. William Bundy and Walter Bonilla

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Gravely Naval Research Group
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

None

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

DISTRIBUTION A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES

A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Gravely Naval Research Group. The contents of this paper reflect my own personal view and are not necessarily endorsed by the NWC or the USN.

14. ABSTRACT

This paper postulates that improvements in technology will transform influence operations in the medium-term future; however, the U.S. will need to take action sooner in order to prevent continued damage to U.S. interests. The U.S. must pursue a two-prong strategy, incorporating technological advances as they become available, while leveraging extant technology into improved doctrine to confront current threats. Critically, the U.S. must leverage the synergies between command of passive information gathering, active narrative shaping, and the transport-layer infrastructure over which information passes.

15. SUBJECT TERMS

Information Operations, IO, Gray Zone, Asymmetry, blockchain, machine learning, intelligent agent, artificial intelligence, cyber, social media

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Dr. William F. Bundy, Director, Gravely Group
UNCLAS	UNCLAS	UNCLAS		45	**19b. TELEPHONE NUMBER** *(Include area code)* 401-841-2674

Reset

The U.S. Needs Trolls:

Strategic Concepts to Command the Gray Zone Struggle
Technology and Doctrine to Revolutionize Influence Warfare

Joshua S. Samet
U.S. Department of State

A paper submitted to the Faculty of the United States Naval War College Newport, RI in partial satisfaction of the requirements of the Gravely Group for Naval Warfare Research elective.

DISTRIBUTION A. Approved for public release: distribution unlimited. The contents of this paper reflect the author's own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

May 23, 2018

Table of Contents

Abstract

This paper postulates that improvements in technology will transform influence operations in the medium-term future; however, the U.S. will need to take action sooner in order to prevent continued damage to U.S. interests. The U.S. must pursue a two-prong strategy, incorporating technological advances as they become available, while leveraging extant technology into improved doctrine to confront current threats. Critically, the U.S. must leverage the synergies between command of passive information gathering, active narrative shaping, and the transport-layer infrastructure over which information passes.

This paper espouses three specific recommendations. First, the formation of an organizational structure modeled after a combination of the Director of National Intelligence Open Source Center, the now obsolete United States Information Agency (USIA), and the French Foreign Legion. Second, implementation of a solution possibly leveraging blockchain to assign trust and relevancy values to news outlets, individual stories, and users. Third, ensure constant reevaluation of the technologies available to the U.S. and her adversaries in the domain of intelligent agents especially.

Introduction

Russian attempts to undermine democratic institutions in the United States and its allies have increased in frequency and effectiveness in recent years. Although the controversy of Russian election meddling during the 2016 U.S. presidential elections has received significant attention, it marked neither the first instance of such meddling nor the latest. While the long-term efficacy of Russian influence operations remains to be judged, the overall sophistication of their tactics, techniques, and procedures, as well as their ability to blend information warfare with other disciplines, suggests that the U.S. needs to remain vigilant. Although the threat posed by Russian information warfare is not yet existential for the United States, the legitimacy of domestic democratic institutions—for the purposes of this paper, the institutions of universal franchise, majority rule, and regular elections—as well as U.S. international relationships are being eroded by narratives created by Russia. A long-term erosion of legitimacy will adversely affect these institutions and relationships and harm U.S. interests.

Changes in technology will greatly impact tactics, techniques, and procedures in both the offensive and defensive spheres of information warfare. Likewise, advances in technology will increase the danger posed by inattention to the problem. Improvements in technology will transform influence operations in the medium-term future; however, action will be needed sooner in order to prevent continued damage to U.S. interests. The U.S. must pursue a two-prong strategy, incorporating technological advances as they become available, while leveraging extant technology into improved doctrine to confront current threats. Failure by the U.S. to fully address either prong of the strategy poses an unacceptable risk.

If the United States allows its adversaries to achieve a level of sophistication, with the addition of emerging technology, to pose an existential threat, it may be too late to recapture the narrative and successfully defend the institutions and relationships it holds dear. If the United States simply adds the weapons of our adversaries to our own repertoire, without looking to the power of emerging technologies, we also risk irreparable harm. Finally, if the United States merely incorporates our adversaries' tactics, techniques, and procedures without thought to our national values or the legal and ethical implications of operating within the gray zone, we risk doing harm to precisely the same institutions we seek to defend.

This paper posits that the United States must develop both defensive countermeasures to Russian perception shaping operations and offensive tactics, techniques, and procedures based on adapting Russian doctrine. These offensive and defensive measures will require multiple levels of effort, both public and discrete, as well as both internationally focused and domestic. They will require a delicate touch to navigate between overreaction, risking conflict with Russia, and underreaction, which incentivizes further attacks. The U.S. must avoid temptation to leverage our adversaries' narratives as political cudgels domestically.

The U.S. must learn from Russian successes and failures in order to craft its defensive and offensive information postures. As the 2017 U.S. National Security Strategy notes, "Russia aims to weaken U.S. influence in the world and divide us from our allies and partners."[1] To understand how to confront this threat, we must learn from it. While employing the exact same methodology may not help the U.S. achieve its domestic of foreign policy goals, a deeper understanding of the phenomenon would allow a smarter, more coherent response. Also, the sophistication and potential provided by Russian successes offers a tempting selection of tools to adapt to our own needs.

[1] Donald J. Trump, "National Security Strategy of the United States of America," White House, December 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf 25–26.

Background

> *"This is another type of war, new in its intensity, ancient in its origin--war by guerrillas, subversives, insurgents, assassins, war by ambush instead of by combat; by infiltration, instead of aggression, seeking victory by eroding and exhausting the enemy instead of engaging him."*[2]
>
> - John F. Kennedy, June 1962

The first step in confronting irregular threats is understanding. While this paper will focus primarily on confronting Russian perception warfare operations against the United States, these operations need to be viewed as but a part of a larger field of study. Attacking the perceptions of decision makers is part of a more nuanced information warfare sphere within the Russian military and security establishment. Information warfare is but a subset of a larger sphere of irregular warfare. Russia is but one of many nations and non-state groups to engage in irregular warfare. While the focus of the historical framing of this paper is strongly focused on Russia, the operational courses of action advocated herein may be used to confront other foes.

The technology which will greatly impact the Russian information warfare apparatus in coming years will not be their exclusive province. The coming revolutions in artificial intelligence and manipulation of massive data sets will allow perception warfare by friends and adversaries alike, as well as by non-state actors, corporate entities, and even individual actors. The resource requirement for such operational activities will be greatly reduced and absent a strong commitment to defensive measures the efficacy of propaganda will increase.

This paper asserts that perception warfare is a component of a larger trend towards gray zone conflict, which the U.S. Special Operations Command defines as "competitive interactions

[2] John F. Kennedy, "Remarks at West Point to the Graduating Class of the U.S. Military Academy." *The American Presidency Project*, 6 June 1962, http://www.presidency.ucsb.edu/ws/index.php?pid=8695

among and within state and non-state actors that fall between the traditional war and peace duality."[3] This trend will continue and intensify in coming years and the United States needs to become more adept at operating within this gray zone. As such, it is imperative to understand how our adversaries see the battlespace.

The Russian Concept of Information Warfare

Although this paper focuses primarily on perception shaping, the Russian concept of information warfare encompasses additional elements. Russia has improved the "combined arms" nature of its information warfare utilizing traditional computer and communication network disruptions to isolate human populations, and perception shaping to fill the information void created. Russia's concept of information warfare was described by author Paul M. Joyal as resting upon three pillars. Roughly summarized, these pillars consist of a phase to acquire information on the opponent and conditions needed to achieve victory, a phase to gain understanding of the opponent's information systems, and a phase to interrupt the enemy's flow of information.[4]

The Russian vision for information warfare is not substantially different from that of the United States. While there is no definitive and openly available documentation of Russian doctrine on information warfare per se, Russian Military Doctrine published in 2010 notes the importance of information warfare to weaken enemy command and control and to create positive international views of the Russian position.[5] U.S. doctrine, as described in Joint Publication 3-13, recognizes that "influence is at the heart of diplomacy and military operations, with

[3] Philip Kapusta, "The Gray Zone." *U.S. SOCOM*, 9 September 2015, https://info.publicintelligence.net/USSOCOM-GrayZones.pdf

[4] Paul M. Joyal, "Cyber Threats and Russian Information Warfare." *Jewish Policy Center (blog)*, Winter 2016. https://www.jewishpolicycenter.org/2015/12/31/russia-information-warfare/

[5] Heickero, "Emerging Cyber Threats and. Russian Views on Information," *Swedish Defence Research Agency*, 2010, http://www.highseclabs.com/data/foir2970.pdf. 12.

integration of [information-related tools or techniques to create operationally desirable conditions] providing a powerful means for influence."[6] The ultimate goal for these efforts is to influence, disrupt, corrupt, or usurp decision making, whether by affecting cognitive processes or the physical paths over which information flows.[7] There are variations in how Information Warfare is implemented, but at their core Russian and U.S. doctrines appear focused on similar outcomes.

Importantly, the Russian concept of operations uses a wide definition of "opponent," to include civilian populations in addition to military and government infrastructure. Russia brings to bear its three pillars against media outlets since they are analogous to military command and control, but on a social-cultural level. Russian doctrine denies the adversary access to external information, and replaces it with a chosen narrative.[8] Chief of Russian General Staff General Samsonov in 1996 contended that the effects of information warfare could be likened to a weapon of mass destruction since technology could "disorganize state administration" and "affect the moral spirit of the population" among other impacts.[9] Russian informational interventions are, simply stated, the act of subverting the social command and control of a nation.

Historical Perspective Informing Russian Activities

Both as a product of U.S. conventional military hegemony following the breakup of the Soviet Union and as a result lessons gleaned from their own successes and failures in information warfare, perception shaping operations are an appealing option for the Russian government to project power. Russian Army Colonel Sergei Modestov, as quoted by author

[6] Joint Chiefs of Staff, "Joint Publication 3-13: Information Operations," 2012. II–2.
[7] Joint Chiefs of Staff, "Joint Publication 3-13: Information Operations," 2012. II-2
[8] Paul M. Joyal, "Cyber Threats and Russian Information Warfare." *Jewish Policy Center (blog)*, Winter 2016. https://www.jewishpolicycenter.org/2015/12/31/russia-information-warfare/.
[9] Heickero, "Emerging Cyber Threats and. Russian Views on Information," 16.

Nikolas Gvosdev, noted in the 1990s that cyber warfare was a means which could be utilized to engage an adversary without resorting to open conflict.[10] This makes information warfare appealing as both a precursor and adjunct to kinetic military actions or a standalone option to further ideologies friendly to Russia.[11] It also allows Russia to operate within the gray zone between war and peace.[12] While U.S. prowess in conventional arms is an effective deterrent to Russian conventional warfare, this same prowess incentivizes irregular warfare as a means to counter perceived U.S. power. Russia views information warfare as a powerful component of irregular warfare.

Several perceived failures influenced Russian views on its current perception shaping operations. Seen through the lens of this Russian view on information warfare, there is little surprise that media-driven social change such as Eastern Europe's 'color revolutions' or the 'Arab Spring' are viewed as a western mechanism for regime change.[13] [14] When U.S. officials speak of 'soft power' and democratization, Russian leadership hears the language of information warfare and sees a threat to Russian influence.[15] An argument could be made that the changed U.S. rhetoric on democratization in the first year of the Trump Administration might serve to assuage fears of ideological strife in the Kremlin; however, there is little evidence that Russian leadership feels less concerned, and the change in Washington's language might have quite a different effect in other European capitals.

[10] Derek S. Reveron, *Cyberspace and National Security*, (Georgetown University Press, Washington, DC, 2012) 176.

[11] Armin Krishnan, *Military Neuroscience and the Coming Age of Neurowarfare*, (Routledge, Taylor & Francis Group, New York, 2017) 185.

[12] Kapusta, "The Gray Zone."

[13] Krishnan, *Military Neuroscience and the Coming Age of Neurowarfare*, 186.

[14] Sebastian Rotella, "Russia's Shadow-War in a Wary Europe." *ProPublica*, April 4, 2017. https://www.propublica.org/article/russias-shadow-war-in-a-wary-europe.

[15] Rotella, "Russia's Shadow-War in a Wary Europe."

In response to weakness relative to the West in conventional military strength, and as a response to ‘soft power’ and ‘democratization,’ Russia has conducted a number of large-scale information warfare campaigns. Strengths and weaknesses of previous campaigns help inform and adjust successive measures. In 2007, Estonia suffered a cyber-attack, which some experts argue marked one of the first implementations of Russian information warfare methodology as a state-on-state attack.[16] The relocation of a Soviet-era statue precipitated the attack, which began as a relatively low-tech and ineffective attack by Russian-inspired cyber activists. The second phase peaked more than a week later and was more sophisticated, consisting of both a botnet-powered distributed denial of service against critical networks and defacement of websites. The attack ended abruptly in what Roland Heickerö from the Swedish National Defence College noted was a decision by the attackers rather than a result of defensive efforts.[17] Russia quickly incorporated the lessons into their paradigm and the following year the world would see a refinement in Russia’s campaign in Georgia.

In Georgia in 2008, Russia demonstrated a more combined-arms methodology in their information warfare activities, and for the first time combined cyber-attacks with a kinetic military campaign.[18] The techniques also changed with the hackers employing more efficient and effective technical tools.[19] Heickerö described hackers well prepared with knowledge of the adversary’s networks, which implied extensive reconnaissance ahead of time.[20] With the understanding of how Russia views information warfare, this conforms nicely to the vision of the

[16] Heickero, “Emerging Cyber Threats and. Russian Views on Information,” 39.
[17] Heickero, 40.
[18] Heickero, 43.
[19] Heickero, 43.
[20] Heickero, 46.

first two pillars: acquisition of information on the opponent and the overall conditions needed to achieve victory and an understanding of the opponent's information systems.

The Asymmetry of the Information Space

U.S. foreign relations are of a different nature from Russia's. For one thing, Russia behaves far more as a unitary decision-making entity when it comes to foreign relations, whereas U.S. relations with its allies are subject to much greater internal domestic divisions. Russian President Vladimir Putin holds a strongly realist view of international relations, and wields a great amount of power within his nation to direct the course of Russian foreign relations.[21] While there is a sense that U.S. outlook may be in the process of transformation, a strong support for the international liberal worldview has been a hallmark of U.S. foreign policy and alliance-building since the end of World War II.[22] This asymmetry of worldview makes it difficult to compete with the Russians at their game. Simply conducting a perception hacking campaign to compete with the Russian narrative risks alienating allies rather than wooing them. The U.S. will require subtler means.

The social topography of the Russian information space is significantly different from that of the U.S. While the internet in Russia connects to the world, it is significantly more insular than in the U.S. Social networks tend to include Russians discussing Russian issues in the Russian language.[23] The U.S. has a more open and connected society and this makes it an easier target. The U.S. constitution enshrines freedom of speech, and U.S. law limits domestic propaganda by the federal government.

[21] Bobo Lo, "An Accident Waiting to Happen." *Lowy Institute*, 25 October 2017, https://www.lowyinstitute.org/publications/accident-waiting-happen-trump-putin-and-us-russia-relationship
[22] Ibid.
[23] Reveron, *Cyberspace and National Security*, 175.

Russia enjoys far more control over the physical network level than do western nations. Russia has followed a two-prong effort to control this physical layer: legal requirements to provide for government monitoring of network traffic, and ensuring ownership of the digital environment by friendly commercial interests.[24] This too provides an asymmetry for the U.S to overcome, as the regulatory and cultural environment makes it difficult and ill-advised to exert this level of control. Likewise, constitutional law limits the government's authority to monitor internet traffic.

Russia utilizes a large number of cyber activists and machine entities to spread its propaganda through online communities and social media. By this manner, Russia can amplify its message by either drowning out competing narratives or promulgating multiple narratives to sow chaos. NATO's deputy secretary-general and a former American ambassador to Moscow Alexander Vershbow, as quoted in the Economist, described the method as "an endlessly changing storyline designed to obfuscate and confuse to create the impression that there are no reliable facts, and therefore no truth."[25]

The Gray Zone

As already noted, Russia views information warfare as a powerful component of irregular warfare. Russia's heavy reliance on irregular warfare methods has pushed it towards what U.S. Special Operations Command (SOCOM) describes as "gray zone conflict."[26] The SOCOM description of the gray zone as "competitive interaction among and within state and non-state actors that falls between the traditional war and peace duality"[27] is an apt one. SOCOM further notes that gray zone conflict is an opaque process where the nature of the conflict, the specific

[24] Joyal, "Cyber Threats and Russian Information Warfare," 178–79.

[25] "The Fog of Wars." *The Economist*, October 22, 2016. https://www.economist.com/news/special-report/21708880-adventures-abroad-boost-public-support-home-fog-wars.

[26] Kapusta, "The Gray Zone."

[27] Kapusta.

parties involved, and policy and legal frameworks under which it is conducted are all ambiguous.[28] It is within this gray zone that Russia has successfully carved out a spot for its perception warriors.

Although Russia has become adept at operating within this gray zone, it is by no means the only party to do so. As the International Security Advisory Board (ISAB) noted in a January 2017 report for the Department of State, China, Iran, and North Korea are all active within this gray zone.[29] As such, it is imperative that any U.S. attempt to confront Russian gray zone tactics be scalable to other theaters, especially since the gray zone theater is ambiguous and often a nation's true adversary is only revealed in hindsight.

One feature which has exemplified Russia's gray zone is the use of cyber activists, colloquially described as "trolls." Almost three years before the February 2018 indictments handed up by a federal grand jury in Washington, DC, alleging that personnel of the Saint Petersburg-based Internet Research Agency conspired to commit fraud associated with the 2016 U.S. elections,[30] the New York Times detailed perception hacking operations by that organization in a June 2015 exposé "The Agency."[31] Even in 2015, Russia's gray zone attacks against the U.S. were nuanced, well-financed, and of a combined arms nature.

The complexity of the implementation of "trolls" by the Russian gray zone apparatus underscores that these are not amateurs or privateers, per se. These are state-backed, well-

[28] Kapusta, "The Gray Zone."

[29] Hon. Gary Hart (et al.), "International Security Advisory Board." *U.S. Department of State*, 3 January 2017, http://www.state.gov/t/avc/isab/266650.htm

[30] Matt Apuzzo and Sharon LaFraniere, "13 Russians Indicted as Mueller Reveals Effort to Aid Trump Campaign." *The New York Times*, 16 Feb. 2018, https://www.nytimes.com/2018/02/16/us/politics/russians-indicted-mueller-election-interference.html

[31] Adrian Chen, "The Agency." *The New York Times*, 2 June 2015, https://www.nytimes.com/2015/06/07/magazine/the-agency.html

resourced professionals. The 2015 New York Times piece detailed a virtual false flag attack against a chemical plant in Louisiana where "trolls" from the Internet Research Agency in Saint Petersburg ascribed an attack, which never occurred in reality, to the Islamic State.[32] The fake attack "was a highly coordinated disinformation campaign, involving dozens of fake accounts that posted hundreds of tweets for hours, targeting a list of figures precisely chosen to generate maximum attention. The perpetrators didn't just doctor screenshots from CNN; they also created fully functional clones of the websites of Louisiana TV stations and newspapers."[33] The fake disaster even had its own troll-created Wikipedia page, citing extant fake references. The New York Times surmised that "[i]t must have taken a team of programmers and content producers to pull off."[34]

The Strategic Impact of Russian Perception Shaping Operations

The elephant in the room is the continuing impact of Russian meddling in the 2016 U.S. presidential elections. It is by now well documented and commonly accepted that Russia took a position in favor of the ultimately victorious candidate in the closely contested election. The information warfare was likely approved by the Russian president, with the intent to undermine public confidence in the U.S. democratic process and help the election of Russia's preferred candidate.[35] The U.S. Office of Director of National Intelligence (ODNI) further emphasized the activities advanced "Moscow's longstanding desire to undermine the US-led liberal democratic order."[36] The ODNI's January 2017 report underscored the "combined arms" nature of the Russian campaign. Russia's information warfare campaign combined covert cyber operations—

[32] Chen, "The Agency."

[33] Ibid.

[34] Ibid.

[35] Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections." *ODNI*, January 2017. Ii.

[36] "Assessing Russian Activities and Intentions in Recent US Elections." Ii.

such as the theft of emails from Secretary Clinton and the Democratic National Committee—with the release of propaganda created from that stolen information.[37]

This Russian effort must be viewed through a special lens. Russia is our adversary and views the North Atlantic Treaty Organization (NATO) and European Union (EU) as threats. Russia is investing in cyber capabilities and technologically advanced forms of subversive tactics.[38] Russia has shown a willingness to interfere in the internal affairs of countries around the world.[39] The threat is simply greater with Russia than with other states or non-state actors. Russia has demonstrated a combination of will and ability to operate in this domain; her intent is more easily defined as hostile and Russia is a capable military foe whose nuclear arsenal deters certain remedies for bad acts.

U.S. response to this point has been weak. The outgoing Obama Administration levied sanctions, to include closing two Russian intelligence-related compounds,[40] but Russian interference in U.S. internal affairs has continued. The Council on Foreign Relations noted in November 2017 that Russian cyber activists were active in stoking the controversy over NFL players' national anthem protests, presumably to fuel discord within American society[41] More recently, Russian propaganda sought to spread discord following a tragic

[37] "Assessing Russian Activities and Intentions in Recent US Elections," ii.
[38] Trump, "National Security Strategy of the United States of America," 26.
[39] Trump, "National Security Strategy of the United States of America," 26.
[40] Greg Miller, Ellen Nakashima, and Adam Entous, "Obama's Secret Struggle to Punish Russia for Putin's Election Assault." *Washington Post*, 23 June 2017, https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/
[41] Keir Giles, "Countering Russian Information Operations in the Age of Social Media." *Council on Foreign Relations*, November 21, 2017. https://www.cfr.org/report/countering-russian-information-operations-age-social-media.

school shooting in Florida in February 2018.[42] If measures taken have been intended as deterrence, they do not appear to be working.

Meanwhile, Russian efforts have targeted our allies. Mounting evidence points to a Russian hand in steering the conversation on social media towards a British decision to exit the European Union[43] and in backing far-right or pro-Russian parties or candidates in France,[44] [45] the Czech Republic,[46] and elsewhere. Russian information operations are backing the smear campaign against Syrian first-responders known as the "White Helmets" by painting the group as terrorists to undermine antiregime forces, including the U.S.[47] [48] Voters in the Czech Republic in January 2018 will cast their votes for president, with the pro-Russian candidate promising a referendum on continued membership in the EU and NATO.[49]

Although it is difficult to differentiate between causes of our partners' diminishing confidence in the United States' resolve to defend our allies, a combination of weak support to NATO by the incoming Trump Administration and a simultaneous narrative of "successful" usurpation of the U.S. democratic process which led to that administration creates a caustic

[42] Sheera Frenkel and Daisuke Wakabayashi, "After Florida School Shooting, Russian 'Bot' Army Pounced." *The New York Times*, 19 Feb. 2018, https://www.nytimes.com/2018/02/19/technology/russian-bots-school-shooting.html

[43] "Russian Twitter Trolls Meddled in the Brexit Vote. Did They Swing It?" *The Economist*, November 23, 2017. https://www.economist.com/news/britain/21731669-evidence-so-far-suggests-only-small-campaign-new-findings-are-emerging-all.

[44] "The Fog of Wars." *The Economist*, 22 Oct. 2016, https://www.economist.com/news/special-report/21708880-adventures-abroad-boost-public-support-home-fog-wars

[45] Sebastian Rotella, "Russia's Shadow-War in a Wary Europe." *ProPublica*, 4 Apr. 2017, https://www.propublica.org/article/russias-shadow-war-in-a-wary-europe

[46] Drew Hinshaw and Philip Heijmans. "Pro-Moscow Candidate Pulls Ahead in Czech First-Round Vote." *Wall Street Journal*, January 13, 2018, sec. World. https://www.wsj.com/articles/czech-election-highlights-allure-of-russia-for-eastern-europe-1515758994.

[47] Emma Grey Ellis, "Inside the Conspiracy Theory That Turned Syria's First Responders Into Terrorists." *WIRED*, April 30, 2017. https://www.wired.com/2017/04/white-helmets-conspiracy-theory/.

[48] Olivia Solon, "How Syria's White Helmets Became Victims of an Online Propaganda Machine." *The Guardian*, December 18, 2017, sec. World news. http://www.theguardian.com/world/2017/dec/18/syria-white-helmets-conspiracy-theories.

[49] Drew Hinshaw and Philip Heijmans, "Pro-Moscow Candidate Pulls Ahead in Czech First-Round Vote." *Wall Street Journal*, 13 Jan. 2018, https://www.wsj.com/articles/czech-election-highlights-allure-of-russia-for-eastern-europe-1515758994

narrative. As author Stephen M. Walt notes, alliances exist in order to increase the security of their participants. That which casts doubt on the will or ability of a participant to support this requirement will impact the relationship.[50] This is not to say that the Trump Presidency is uniquely to blame for U.S. allies' doubts, but in the wake of George W. Bush's failure to strongly support Georgia against Russian aggression and the Obama Administration's relatively anemic defense of Ukraine, the specter of a U.S. president placed in office with the Kremlin's assistance, who pointedly failed to reaffirm U.S. commitment to NATO's precept of mutual defense,[51] cannot help but add to these fears.

Options to Respond

Before considering possible options to respond, this paper will briefly consider the question of "why not do nothing?" There are several possible hypotheses which could argue for inaction. Are current efforts sufficient to defend democratic institutions and partner relationships? Do successful Russian gray zone attacks really pose a significant threat to the same? Is corporate America capable of adapting to the pressures without government or military response? Do the risks of action outweigh the risks of inaction?

At the risk of being glib, we have been over much of this already. The evidence already cited suggests that current efforts are not sufficient, and these gray zone attacks pose an unacceptable risk. As for whether corporate self-regulation is capable of confronting this issue, I would recall Cathy O'Neil's sage observation when discussing Facebook and other tech

[50] Stephen M. Walt, "Why Alliances Endure or Collapse," Survival, Spring 1997, 160.

[51] Susan B. Glasser, "Trump National Security Team Blindsided by NATO Speech." *Politico*, June 5, 2017. https://www.politico.com/magazine/story/2017/06/05/trump-nato-speech-national-security-team-215227

companies: “they’re focused on making money.”[52] O’Neil continues that our government regulates these companies, and their profits are dependent on the level of this regulation. These companies hire lobbyists and pay into the political system in the form of political contributions; however, these companies now represent something different than classic corporate entities because they can shape political behavior of their users and theoretically shape social and regulatory behavior as a result.[53] Corporate America must not be left to deal with this without supervision.

The final question, whether the risks of action outweigh those of inaction, is much more difficult to answer. The risks of inaction have already been described, continued actions on the part of our adversary to influence the perceptions of U.S. and allied populations, leading to a gradual degradation of U.S. institutions and relationships. Since these institutions and relationships are key U.S. interests, the cost of inaction is high. On the other hand, the cost of action is very hard to quantify. There is a cost in resources, but this is not as powerful a concern as the nature of gray zone conflict vis-à-vis the narrative of a nation that bases its narrative on democracy and personal freedoms.

This paper suggests adherence to the values, narrative, and principles of the U.S. is critically important and must be considered in depth when evaluating courses of action. These same values, narrative, and principles should not be used as an argument for inaction. The stakes are high and we must respond. To that end, this paper lays out three options to leverage technology or changes in force structure to address the problem.

[52] Cathy O’Neil, *Weapons of Math Destruction*, (Crown, New York, 2016) 181.
[53] O’Neil, 180–81.

General Concept

At its most simplistic, this paper proposes a concept of action that relies heavily on constructing an institutional and bureaucratic framework conducive to confronting the problem described rather than specific technology-driven remedies. The framework must be sufficiently agile to incorporate technological advances, to include autonomous or "intelligent" systems, but must not focus exclusively on the technology to define the solution. The solution instead should focus on creating and maintaining cross-cutting institutions capable of targeting and executing strategic informational fires and countering those of our adversaries.

That is not to say that technology will be unimportant to this effort, but rather that the impact of particular technologies on information warfare in the decades to come is difficult to predict. This paper maintains that cognitive computing offers both opportunity and threat in this realm and that the possibility exists that within 20 years today's model of cybersecurity will be turned on its side: the concept of machines hacking human cognition will likely come to pass. The model has been tested to the point described already, where machines are used as intermediaries through which humans hack the cognition of other humans. The real question is how much the process can be automated and when this automation will occur. It must be emphasized, however, that whether machines hack humans or humans hack humans is academic. The hacking is occurring. Automation will continue. The framework by which we respond to this is what is important, not the specific technologies employed.

These frameworks and institutions must combine a deep understanding of, and capability to control, the networks over which information moves with an equally strong command of the underlying material which comprises the information. This latter aspect of the challenge is likely the most demanding, since it is ultimately the feature which acts upon the human cognition we are attempting to protect or attack. It involves both a passive presence in the information space and an active creation and delivery of content.

Enter the Troll Legion

Much of Russia's influence campaign is powered by cyber activists of Troll Farms. While an exact copy of this method is probably not a good fit for U.S. sensibilities, law, and image, the outcome has been sufficiently powerful to warrant exploration as a possible way forward. The advantages of troll farming include: plausible deniability, cost savings, contingency capacity. Disadvantages include a softness of command and control relationships and difficulty ensuring adherence to training and doctrine requirements.

While troll farms resemble a 21st century institution modeled after privateers of old, this paper proposes an institution more in line with the French Foreign Legion. It could also be viewed as somewhat similar to the model employed by the U.S. Director of National Security's Open Source Center, formerly known as the Foreign Broadcast Information Service (FBIS). In a 1992 speech by J. Niles Riddel, the deputy director of the Open Source Center's predecessor noted that field activities were staffed by a combination of U.S. and foreign national personnel and generally functioned as part of a U.S. diplomatic mission or military command. These activities operated with the full knowledge and consent of the host government.[54] By 1992, FBIS operated a network of 19 regional bureaus for collection, processing, and distribution of open source information in their respective geographic areas.[55] Under this paradigm, foreign nationals with native linguistic ability and cultural familiarity monitor open source reporting,

[54] J. Niles Riddel, "Remarks by J. Niles Riddel, Foreign Broadcast Information Service." *Federation of American Scientists,* 2 December 1992, https://fas.org/irp/fbis/riddel.html

[55] Kalev Leetaru, "The Scope of FBIS and BBC Open-Source Media Coverage, 1979–2008 (U)." *Studies in Intelligence,* March 2010, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/volume-54-number-1/PDFs-Vol.-54-No.1/U-%20Studies%2054no1-FBIS-BBC-Coverage-Web.pdf

providing summaries to staffers who select which items are translated and processed further.[56] This paradigm would work well to model U.S. Cyber Legion 1.0.

The French Foreign Legion, by contrast, is a more purely military organization. Recruits enter initial contracts with the Legion a period of 5 years, with follow on contracts varying from 6 months to 5 years.[57] Recruits to the Legion may be either French or foreign and may apply for French citizenship after three years of honorable service. The Legion, as currently constituted, is primarily stationed domestically with the only units permanently based outside France the 3rd Infantry Regiment in French Guyana and a detachment in Mayotte (a French possession in the Indian Ocean).[58] In this respect, The U.S. Cyber Legion would be different. The focus would be on the abroad. Recruitment, training, and deployment would be focused on regional centers.

Another organization to look to for precedent is the United States Information Agency (USIA), which existed from 1953 to 1999 as the U.S. government entity under which all overt foreign information activities were conducted.[59] While possibly best known as the organization under which Voice of America operated, USIA also managed cultural and educational exchanges, ran overseas libraries, and coordinated film programs. Over time, the organization's mandate shifted to reflect new media technologies, but its core mission was to express the informational message of the U.S. government to audiences abroad.[60] This would be an important piece of the mission of U.S. Cyber Legion 1.0.

[56] Riddel, "Remarks by J. Niles Riddel, Foreign Broadcast Information Service."

[57] "French Foreign Legion Recruitment." *French Foreign Legion Website*, 2 March 2018, http://en.legion-recrute.com/

[58] "French Foreign Legion Recruitment."

[59] "Records of the United States Information Agency (RG 306)." *National Archives*, 15 Aug.2016, https://www.archives.gov/research/foreign-policy/related-records/rg-306

[60] "Records of the United States Information Agency (RG 306)."

This troika of organizational models provides a starting place to envision a new organization. Like FBIS, the organization would need to be linguistically and culturally attuned to the target battle space. It would need to work in a somewhat passive mode, like FBIS, to monitor media messaging. As social and technical patterns shift with time, the new organization would need to shift to remain relevant. Like with USIA, the new organization would have to manage the outward flow of information and messaging in real time. Like with the French Foreign Legion, the new organization would need to operate under appropriate authorities to confront adversaries within the gray zone of conflict. The central goal within the gray zone is to avoid war, but the stark reality is that our actions within this sphere will be seen as information warfare. This is true of Russia and likely true of any other adversaries we chose to confront in this manner. The new organization will be military and must be able to exercise the appropriate authorities to accomplish its mission.

One option would be to run the new organization jointly as subordinate to both SOCOM and U.S. Cyber Command (USCYBERCOM) with integrated support from across the intelligence community. In the French Foreign Legion, officers of the French Army make up most of the leadership cadre, with only about 10 percent of officers coming from the ranks of the Legion's non-commissioned officers or veterans.[61] The U.S. Cyber Legion 1.0 would similarly be led by a commissioned officer corps of U.S. citizen military professionals. A smaller proportion of foreign troops could be expected to qualify for leadership positions once naturalized as U.S. citizens.

[61] "Un statut particulier." *Legion Etrangere*, 28 Février 2018, http://www.legion-etrangere.com/mdl/info_seul.php?id=81&block=27&titre=Statut-du-legionnaire

The U.S. Cyber Legion 1.0 model, as proposed in this paper, would offer better command and control and more rigid adherence to training and doctrine than employing privateers, but at the cost of a level of plausible deniability. This model would still require a parallel structure for situations requiring true clandestinely, but would allow flexibility and cost-effective options for a large number of cases where associating a message with the U.S. government poses little risk.

Finally, it deserves to be underscored again that this function is inherently military and to succeed in the gray zone, we will need to deliver combined effects on target, including at times kinetic effects. As aptly noted on “Hamilton 68,” a website created by Alliance for Securing Democracy that tracks activity of Twitter accounts identified as Russian propaganda vectors: “any effort to block fake news will ultimately lead to infringements of freedom of speech and the press. We believe a better approach focuses on the producers of disinformation rather than their output.”[62] If informational fires are insufficient to suppress or deter these producers and if network-layer fires are similarly insufficient, there are times when kinetic response will be required. The gray zone is complicated and information alone will not always take the day.

Blockchain Revolution

One frailty of the current information domain is the ease by which bad actors can insert false news to change the outcome of decisions. While this paper will not dwell on the mechanisms to improve the trustworthiness of press, there is merit in a short discussion of blockchain technology as a possible option to provide insight into the validity of a particular piece of reporting. Blockchain holds potential to add to society’s arsenal to support the spread of valid and verifiable information, while highlighting “fake news” as such.

[62] “Hamilton 68.” *Hamilton68: Tracking Russian influence operations on Twitter*, 16 Feb 2018, http://dashboard.securingdemocracy.org/

Citizens must be given better tools to evaluate the value and accuracy of information they receive. One group looking at blockchain to provide such a tool is Userfeeds, a protocol designed to give information consumers an ability to crowdsource assessments on relevancy and accuracy of material.[63] The protocol would be implemented at the platform-level by social media or other information provider and includes "proof-of-evaluation" and a social "reputation" measure for users.[64] Userfeeds itself underscores that falling expense of creation and transmission of content has placed the burden of evaluation on the recipient of the information rather than the sender.[65] This situation begs for a technological tool to free humans to focus on relavent and accurate information. Userfeeds and other groups propose using blockchain to track stories and the value-assessments of their readers.

These value-assessments need to be stored and maintained in such a way to prevent tampering. Blockchain is one of the technologies underpinning cryptocurrencies such as Bitcoin but has other use cases for tracking transactions in an immutable and publicly scrutinized manner.[66] One set of transactions that could plausibly be tracked and recorded would be those trust and relevance transactions associated with individual journalistic output, journalists, media outlets, individual users, et cetera. In such a manner, trust values for actors in the information domain could be recorded, accessed, and tracked in the same manner as financial transactions.

Intelligent Agents

The realm of technology involving machine cognition, intelligent agency, artificial intelligence, and the myriad of other terms until recently were the province of science fiction

[63] Steven Buchko Buchko, "Blockchain's Fight Against Fake News." *CoinCentral.com*, 26 March 2018, https://coincentral.com/blockchains-fight-against-fake-news/

[64] Buchko

[65] "Userfeeds Protocol Whitepaper [Draft]." *Userfeeds.io*, May 2018, https://userfeeds.io/Userfeeds_Protocol_Whitepaper_[Draft].pdf

[66] Zoran Lalic, "A Deep Dive into Blockchain and Bitcoin." *Insecure Magazine*, March 2018, https://www.helpnetsecurity.com/dl/insecure/INSECURE-Mag-57.pdf

novels rather than joint doctrine publications. This will change rapidly as technology advances. It is as difficult to predict the scope of these advances or their consequence to information warfare 20 years out as it would have been in 1998 to estimate the impact of Facebook on U.S. voter turnout. The premise of this paper is not to offer specific predictions, other than that technology with information warfare implications will advance rapidly and the U.S. must position itself to leverage these advances.

Looking to the medium-term future, antiquated vision of "hacking" within the cyber domain will be turned on its side. In recent decades, the model goes something like this: human cognition, through a machine interface and transport-layer, influences the behavior of machines against the will of those machines' masters. We are already on the cusp of a revolutionary change in this model. In the future, machines will hack back through that transport-layer and machine interface to influence human cognition and behavior. This influence will be effected against the conscious will of the human cognitions involved, and often without the knowledge of those humans.

This process is already taking place. During the 2010 and 2012 elections, Facebook studied whether their platform could influence voters to turn out to the polls. This study using a tool they termed "voter megaphone" leveraged peer pressure to encourage citizens to vote by showing that their friends had voted. Researchers estimated the study involving 61 million users increased turnout by 340,000.[67] If this increase in turnout were distributed unevenly between political parties or interest groups, the outcome of many races could have been changed. The future is not yet upon us since we are still reliant upon human cognition, through a machine interface, transport-layer, and algorithms for analysis, to hack the cognition of other humans.

[67] O'Neil, *Weapons of Math Destruction*, 280–81.

We are getting close, however, and this study must offer a warning that as automation increases and computers get “smarter” and more powerful, fewer humans will be able to profoundly influence the outcomes of society’s decisions.

Algorithmic decisions of social media providers act as gatekeepers to news and political content and directly influence decisions by users. Facebook took their studies of political impact a step farther in 2012 when a researcher changed the newsfeed algorithm of 2 million politically engaged users to include more hard news and less fluffy personal stories from friends’ posts. The study showed a 3 percent rise in voter participation.[68] Two questions present themselves here: what if Facebook had chosen to influence only “liberals,” “Latinos,” or “gun rights advocates” instead of a more neutral group of the “politically engaged?” What if Facebook had acted as an editorial gateway in deciding what hard news to present to this user group? In either case, the 3 percent increase in voter participation would have favored one political position over another.

As an offensive informational weapon, the power of social media and the big data underpinning it is striking. The question becomes how to weaponize the medium to allow the U.S. to influence the cognitive processes of our adversaries? The studies looking at Facebook are useful, but it should be cautioned that in the Russian Republic Facebook and Twitter were only the fourth and sixth most used social media platforms as of November 2017. The most visited social media platform in Russia is the site “VKontakte,” which is popular with younger Russians.[69] As with Facebook, VKontakte (or VK) allows users to add friends, followers, photos, and links to news content. It also allows companies to add content for marketing

[68] O’Neil, *Weapons of Math Destruction,* 282.

[69] Maksim Komonov, Komonov, “100 Million Russians Use Social Media Every Day.” *Practical Ecommerce*, 2 November 2017, https://www.practicalecommerce.com/100-million-russians-use-social-media-every-day

purposes. VK is geared toward users from former Soviet republics in Eastern Europe, particularly Russians, and claimed over 70 million daily users and 3 billion page views each day as of August 2017.[70] The website Odnoklassniki is used by middle-aged Russians, between 34-45, and is the third most popular social media platform in Russia (after VK and YouTube).[71] One key prerequisite to successfully weaponizing the cognitive domain is understanding where human cognition congregates.

An obstacle to U.S. action will be the asymmetry of Russian control of their physical information space. As already noted, Russia requires companies to provide for government monitoring of network traffic and ensues ownership of the digital environment by friendly commercial interests.[72] Russian Internet giant Mail.ru owns VK and as such, VK follows Russian laws.[73] This means that Russia is far more able to monitor and inject influence into the platforms where its population congregates than the U.S. is into its domestic platforms. The asymmetry can be taken one step further: Russia enjoys far more unfettered access into U.S. social networks than the other way around.

Thus, the U.S. starts at a disadvantage structurally. One possible remedy to this disadvantage is to take advantage of Russia's desire to exercise its sphere of influence in Eastern Europe. If we successfully implement U.S. Cyber Legion 1.0, and continue to incorporate technology advances, it could be useful to run the upgraded U.S. Cyber Legion 2.0 from a location within this sphere, e.g., Poland, Ukraine, or Romania. Even so, Russia takes this matter seriously, and in January 2018 a Russian appeals court overturned a lower court ruling and held

[70] Kira Kirk, Kirk, "What Is VK and Why Should You Care?" *Echosec*, 25 Aug. 2017, https://www.echosec.net/what-is-vk-and-why-should-you-care/

[71] Komonov, Komonov, "100 Million Russians Use Social Media Every Day."

[72] Kapusta, "The Gray Zone."

[73] Kirk, "What Is VK and Why Should You Care?"

that only VK has the right to mine VK's data.[74] Thus, a forward presence does not negate the Russian structural advantage, but it may prove to mitigate that advantage as the human element becomes less critical and the intelligent agent technology becomes more mature.

One challenge then for the U.S. is to successfully conduct microtargeting of specific groups within Russia, despite the already noted structural disadvantage. An example would be the ability for U.S. informational fires to target 25-35 year-old urban Russians who support press and individual freedoms, while not opposing the Putin regime. These informational fires could avoid targeting, for instance, Putin hardliners that might be offended by the content. These are similar tactics being used in the U.S. by specific interest groups. In 2015, an analogous campaign was enacted by an anti-abortion group where a doctored video purportedly damning to Planned Parenthood was microtargeted to specific users, while largely trying to avoid the scrutiny of a mass market. The video succeeded in raising money for the anti-abortion group from microtargeted populations for whom the issue was salient.[75] This task is made substantially harder by maintaining the raw dataset in the hands of the Russian corporate entity.

Another challenge for the U.S. is to defend against microtargeting by adversarial states, groups, and individuals. The danger posed by this scenario was on stark display in March 2018 when it was revealed that a UK-based firm, Cambridge Analytica, improperly obtained a large dataset of Facebook user data including the very information useful in microtargeting: identities, friends, "likes," et cetera.[76] The information was obtained 2014 when such acts were not prohibited by Facebook's terms of service and the social media giant has since banned the

[74] "Vkontakte Wins an Appeals Lawsuit against Third-Party Data Mining." *Meduza*, 30 January 2018, https://meduza.io/en/news/2018/01/30/vkontakte-wins-an-appeals-lawsuit-against-third-party-data-mining
[75] O'Neil, *Weapons of Math Destruction*, 193–94.
[76] Kevin Granville, "Facebook and Cambridge Analytica." *The New York Times*, 19 March 2018, https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

practice,[77] but the relative ease by which Cambridge Analytica came by the trove of data should give us pause. The breach, if it can be called that, underscores certain harsh realities of free, capitalist societies. Information has value and corporate entities collect, aggregate, and process these large datasets in order to monetize the information. While corporate behavior can be compelled by regulation, the bottom line takes precedence over national interest. The needs of the user, or even the society writ large, are a distant afterthought.

The Cambridge Analytica bulk data scandal had tenuous connections to Russia, but whether the data itself made it to Russian hands is irrelevant. The incident underscored the ease by which large datasets can be obtained. The Guardian reported that Aleksandr Kogan, the academic from Cambridge University behind gathering the Cambridge Analytica data, held a teaching position at an academic institution in St. Petersburg, Russia, and obtained grants for research into social media network. Energy firm Lukoil, in 2014, saw a presentation on Cambridge Analytica's work on suppressing voter turnout in Nigeria, and microtargeting social media users during elections.[78] The Facebook data from tens of millions of users was obtained in a deceptively simple manner. Users were asked to download an application allowing them to take a personality survey. The application scraped private information from the users and their friend network on the site.[79] The ease by which this information was lifted from Facebook's servers, the time between transfer and discovery, and the scale of the breach make it likely that this was not an isolated incident. If fact, it is highly likely that had Cambridge Analytica not

[77] Granville.

[78] Carole Cadwalladr and Emma Graham-Harrison, "Cambridge Analytica." *The Guardian*, 17 Mar. 2018, http://www.theguardian.com/news/2018/mar/17/cambridge-academic-trawling-facebook-had-links-to-russian-university

[79] Granville, "Facebook and Cambridge Analytica."

been involved with the very high-profile 2016 U.S. elections, their downfall would not be news today.

For offensive operations, the U.S. must prioritize the theft of large datasets from our enemies. In 2014, hackers obtained and successfully exfiltrated the Office of Personnel Management files of 4.2 million current and former U.S. government employees, security clearance background investigation information for 21.5 million individuals, and fingerprint files for 5.6 million persons.[80] Likewise, in 2017, consumer credit giant Equifax lost data of 147.9 million Americans to hackers.[81] These cases underscore the feasibility of pilferage as a mechanism to obtain raw data against which intelligent agents and algorithmic models can be trained. It should be noted that any of the three datasets mentioned, the Facebook user data, OPM information, or Equifax files, would provide a fertile place to begin microtargeting. The synergy possible between the large datasets which can be obtained by theft, and microtargeting discrete populations should also underscore the importance of combining the passive and active elements proposed in U.S. Cyber Legion 1.0.

Once the data is acquired, U.S. Cyber Legion 2.0 requires more than competent human trolls with a deep understanding of the adversary's society, culture, and inclinations. The sheer size of the datasets involved will necessitate automation to effectively employ. There is an ever-increasing amount of automation taking place in the information space, and additional

[80] Hon. Jason Chaffetz, "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation." *Committee on Oversight and Government Reform U.S. House of Representatives 114th Congress*, 7 September 2016, https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf

[81] Brian Fung, "Equifax's Massive 2017 Data Breach Keeps Getting Worse." *Washington Post*, 1 Mar. 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/equifax-keeps-finding-millions-more-people-who-were-affected-by-its-massive-data-breach/

automation will continue at a frenzied pace. Machines can already translate media material[82] and write automated copy for publication.[83] These feats would have been unthinkable 20 year ago when most of the world was barely out of the typewriter age. The capabilities of cognitive computing 20 years hence will be unimaginable from today's perspective; however, though specific prognostications may be futile, the enduring fact is we must invest in the research and the organizational structure to ensure our ability to leverage large datasets grows along with our access to the data.

One technology worth investigating is that of "bots." Russians and others extensively utilize automated software colloquially termed "bots" to amplify human-created messages. Recognizing these bots as what they are is not trivial, but is largely possible over time. In a February 2018 article, the Economist noted that it is difficult to estimate the number of bots on Twitter's platform, especially newer more sophisticated bots.[84] Researchers from University of Southern California and Indiana University estimated in a study released in March 2017 that 9 to 15 percent of Twitter accounts were bots.[85] The increasing sophistication of artificial intelligence programing will make bots more robust and bot countermeasures more challenging.

Determining which entity controls specific bot accounts is exceedingly difficult using publicly available datasets. The primary parties with capacity to identify bot and troll accounts are the social media companies themselves. Analysts with access to public datasets have an

[82] "Machine Translation - Microsoft Translator." *Microsoft.com*, 6 May 2018, https://www.microsoft.com/en-us/translator/mt.aspx

[83] Corinna Underwood, "Automated Journalism - AI Applications at New York Times, Reuters, and Other Media Giants." *TechEmergence*, 22 June 2017, https://www.techemergence.com/automated-journalism-applications/

[84] "Russian Disinformation Distorts American and European Democracy - Turning Politics up to 11." *The Economist*, 22 Feb. 2018, https://www.economist.com/news/briefing/21737297-mueller-indictment-reveals-some-kremlins-tactics-russian-disinformation-distorts

[85] Onur Varol et al., "Online Human-Bot Interactions: Detection, Estimation, and Characterization." *Indiana University*, March 2017, https://arxiv.org/pdf/1703.03107.pdf

uphill battle to utilize statistical methods to identify suspicious accounts, especially for Facebook, which is a more closed network.[86] This allows a degree of plausible deniability for U.S. Cyber Legion 2.0.

Technology advances will revolutionize information warfare. The quality of natural language content creation will improve, rendering it more difficult to identify bots. Account creation will become more automated. Human curators of the bot armies will be able to adeptly control a larger and larger number of individual machines. Bots will get better with AI assistance. The leadership cadre of bots will automate those tasks currently requiring live trolls. The tasks which can be automated will expand. On the other hand, technology will provide weapons to confront these entities too, but the United States must invest in defense lest it fall too far behind.

Promoting Resiliency

Effectively mitigating Russian perception warfare will require involvement of the U.S. government, foreign partners, private corporate and educational institutions, and individuals. Although recent action by tech giants Facebook and Google to confront this problem are encouraging, a viable solution must extend beyond corporations whose financial interests may not align with the needs of the wider society. In an October 2017 press release, Facebook touted a feature being tested to give users additional context on the articles they see on their social media accounts. The new feature displays "publisher Trust Indicators" using ratings established by the Trust Project,[87] an international association of media and digital companies hosted by

[86] "Russian Disinformation Distorts American and European Democracy - Turning Politics up to 11."
[87] Andrew Anker, "Launching New Trust Indicators From the Trust Project for News on Facebook | Facebook Media.", Nov. 16, 2017, https://media.fb.com/2017/11/16/launching-new-trust-indicators-from-the-trust-project-for-news-on-facebook/

Santa Clara University's Markkula Center for Applied Ethics.[88] The efficacy of this measure is yet to be proven and to succeed, the indicators themselves must be both meaningful and accurate. Additionally, individuals must heed them.

The digital tools used by the Russian information warfare machine are similar to those used by celebrities to boost their cache or commercial concerns to boost the prominence of their products. These tools have come under increasing scrutiny in the U.S. and elsewhere. The State of New York in late January 2018 began investigating a company for selling fake social media followers.[89] Many of the automated accounts sold by the company used the personal information of Twitter users, and some may have been active for years acting to amplify and promote the narratives of the customers of the company being investigated.[90] Although Twitter emphasized the activities in question violated its terms of service,[91] it must be recognized that social media companies monetize their platforms as a function of their user base. Active "bot" accounts are a positive for Twitter and Facebook until they draw public scrutiny or the threat of regulation.

The United States government, and more importantly the individuals who make up the United States government, must encourage a society that is tolerable when viewed in the mirror that is Russian propaganda. Scott Lucas, professor of international politics at the University of Birmingham, noted "[t]he most effective propaganda is when you find someone who believes it then give them support – you don't create them from scratch."[92] In other words, it is much easier to weaponize the truth than a lie. This phenomenon was on display following the

[88] "Frequently Asked Questions – The Trust Project." *The Trust Project,* accessed 31 Jan 2018, https://thetrustproject.org/faq/#what_does_it_do

[89] Nicholas Confessore, "New York Attorney General to Investigate Firm That Sells Fake Followers." *New York Times*, Jan. 27, 2018, https://www.nytimes.com/2018/01/27/technology/schneiderman-social-media-bots.html

[90] ibid.

[91] ibid.

[92] Olivia Solon, "How Syria's White Helmets Became Victims of an Online Propaganda Machine." *The Guardian*, 18 Dec. 2017, http://www.theguardian.com/world/2017/dec/18/syria-white-helmets-conspiracy-theories

February 2018 shooting at a Florida high school. Sites tracking propaganda trolls and their allied bots noted an increase in activity on the subject.[93]

Those seeking to corrupt U.S. democratic institutions from within and those seeking to divide American society for political ends take heed: expect to be caught and expect to damage U.S. interests when those dealings become known. Malfeasance for domestic political ends will be inevitably woven into the narrative that Russia and other adversaries proselytize, namely that U.S. and western democracies are flawed and those in power use underhanded means to remain in power. This narrative is often given credibility by the underlying contradictions in American society rather than as a function of propaganda alone.

One potential way to assist society in developing resilience to propaganda messaging is to shine light on which messages are specifically designed to influence, rather than simply inform. This method works even better when combined with attribution. It is far easier to put a narrative in context when presented that background. As such, programs like RoBhat Labs' Botcheck.me website offer potential to provide such context. The website was created by two University of California, Berkeley students to track known political propaganda Twitter bots. The site tracks the top two-word phrases used by these known bots in a 24-hours period. In the 24 hours following the 14 February 2018 school shooting in Florida, all the leading phrases other than the U.S. President's name were related to the tragedy and included "School shooting, gun control, high school, Florida school."[94] The top hashtags were similarly related to the events in Parkland, Florida.[95]

[93] Erin Griffith, Griffith, "Pro-Gun Russian Bots Flood Twitter After Parkland Shooting." *Wired*, 15 Feb. 2018, https://www.wired.com/story/pro-gun-russian-bots-flood-twitter-after-parkland-shooting/
[94] "Detect and Track Political Bots on Twitter." *Botcheck.me*, Accessed 2 March 2018, https://botcheck.me/
[95] "Detect and Track Political Bots on Twitter."

One of the creators of Botcheck.me, Ash Bhat, noted that sometimes the puppet masters controlling the bots drove the content creation, using their automation to amplify the themes until they are adopted by human users. Other times, the bots insert themselves into existing conversations to take control of the narrative and amplify a chosen message. Mr. Bhat noted it was difficult for social media companies to police conversations once the general public had become a participant in the conversation.[96]

In the long term, a better option is for the U.S. to renew its focus on education. While America remains a leader in higher education, to the envy of much of the world, these educational opportunities remain largely the province of an elite class. The 2017 National Security Strategy proposes efforts to "Promote American Resilience," and even stipulates that "actors such as Russia are using information tools in an attempt to undermine the legitimacy of democracies."[97] Yet, the priority actions outlined in the document focus on short-term solutions. Ultimately, fostering critical thinking and critical reading in U.S. citizenry enhances their ability to navigate an increasingly complex information sphere. Likewise, a prosperous society will provide a smaller attack surface for propaganda and those same critical skills may well bolster national prosperity.

Our European allies have instituted programs along these lines. Sweden, for example, launched a program to teach students to identify Russian propaganda and their Defense Ministry formed special units to identify and counter Russian information intended to undermine Swedish society.[98] Lithuania has a group of citizen-activists who work together to identify and counter

[96] Griffith, Griffith, "Pro-Gun Russian Bots Flood Twitter After Parkland Shooting."

[97] Trump, "National Security Strategy of the United States of America," 14.

[98] Dana Priest and Michael Birnbaum, "Europe Has Been Working to Expose Russian Meddling for Years." *Washington Post*, June 25, 2017, sec. Europe. https://www.washingtonpost.com/world/europe/europe-has-been-working-to-expose-russian-meddling-for-years/2017/06/25/e42dcece-4a09-11e7-9669-250d0b15f83b_story.html.

the vectors of Russian disinformation on social media.[99] The European Union enlisted hundreds of volunteer academics, researchers, and journalists to circulate examples of non-factual propaganda in a weekly digest published in multiple languages.[100]

In the shorter-term, the National Security Strategy's call for information sharing strikes a chord, but that vision should be expanded to include a broader sampling of stakeholders. The vision should include more than simply protecting information. The document states that the U.S. should "improve the coordination among the private sector and all levels of government that is needed to improve resilience, [the U.S.] must make a stronger commitment to protecting sensitive information so that all partners actively identify and share vulnerabilities and work collaboratively to reduce them."[101] The "private sector" should include the U.S. population as well and the information sharing must include informational threats to public perception, rather than simply information systems and technology.

This measure would contrast sharply the policies of the Obama Administration in the run up to the 2016 election. Public disclosure of the scope of Russian attempts to influence the outcome of the U.S. elections was minimal prior to election day. According to the Washington Post, the FBI detected attempts to penetrate 21 state election systems,[102] in addition to the increased hacking activity against those involved in the U.S. election process. Many of the disclosures made since the election were known well before, but either not released to the public or released in piecemeal fashion, even once the scope of the Russian involvement was known within the administration.

[99] Dana Priest and Michael Birnbaum, "Europe Has Been Working to Expose Russian Meddling for Years." *Washington Post*, 25 June 2017, https://www.washingtonpost.com/world/europe/europe-has-been-working-to-expose-russian-meddling-for-years/2017/06/25/e42dcece-4a09-11e7-9669-250d0b15f83b_story.html
[100] Priest and Birnbaum.
[101] Trump, "National Security Strategy of the United States of America," 14.
[102] Miller, Nakashima, and Entous, "Obama's Secret Struggle to Punish Russia for Putin's Election Assault."

The Obama Administration by no means holds a monopoly on this viewpoint. Following a September 2016 briefing to 12 key members of Congress, opinions on whether to publicly release information related to the Russian efforts split along political lines: Democrats called for release, while Republicans resisted, arguing that disclosure would undermine confidence in the election system.[103] Then candidate Donald J. Trump used the situation to further his political motives in July 2016 when he called on Russia to find Hillary Clinton's missing emails. Trump continued, "I think you will probably be rewarded mightily by our press"[104] before praising the Russian president and disavowing Russian connections. Representative Adam Schiff (D-California) noted to the Washington Post that many U.S. groups inadvertently incentivized Russian meddling with their collective focus on mining the ill-gotten booty of hacked emails rather than persuading Americans "why they should care that a foreign power is meddling in our affairs."[105]

The efforts taken under the guise of protecting public confidence in the election system likely had the opposite effect. While possibly well intentioned to protect public perceptions, President Barack Obama desired to avoid publicly politicizing the Russia issue. As noted in the Washington Post, the perception was that it "had the opposite effect: It meant that he allowed politics to shape his administration's response to what some believed should have been treated purely as a national security threat."[106] Likewise, arguments that disclosure risked compromise of intelligence sources and methods have largely been proven irrelevant in hindsight since the information ultimately became available through formal release or otherwise.

[103] Ibid.

[104] Ashley Parker and David E. Sanger, "Donald Trump Calls on Russia to Find Hillary Clinton's Missing Emails." *The New York Times*, July 27, 2016, sec. Politics. https://www.nytimes.com/2016/07/28/us/politics/donald-trump-russia-clinton-emails.html.

[105] Miller, Nakashima, and Entous, "Obama's Secret Struggle to Punish Russia for Putin's Election Assault."

[106] Ibid.

Western democracies must shine a light on Russian meddling. The U.S. has the opportunity, due to its technological position among these western democracies, to lead this effort. The Council on Foreign Relations recommended strongly in November 2017 that "western governments should swiftly and decisively denounce Russian information activities as soon as they are identified, and their counterintelligence agencies should identify quantitative means to measure the effectiveness of Russia's methods."[107] While it is neither desirable or realistic to micromanage the fact-checking of media content or abridge personal freedoms in order to silence propaganda-like sources, a wider push to correctly attribute informational flows would be welcome.

Conclusion

In the end, it comes down to securing the enduring national interests of the United States. If these interests include multilateral security partnerships and maintaining a robust domestic democracy, the U.S. must develop better strategies to counter the Russian propaganda machine. While the needed steps to strengthen alliances and reassure allies are different from those to strengthen democratic institutions and reassure U.S domestic population, they confront the same enemy. That enemy seeks to divide and sow mistrust.

The U.S. must learn from Russian information warfare techniques, but simply adopting these techniques will neither serve domestically nor internationally. We must carve out a solution which matches the values we share with our western allies. The solution must serve to comfort wavering friends, deter our adversaries, and assure our domestic population. This

[107] Keir Giles, "Countering Russian Information Operations in the Age of Social Media." *Council on Foreign Relations*, November 21, 2017. https://www.cfr.org/report/countering-russian-information-operations-age-social-media.

should be done in a manner which does not unduly back Russia into an isolated corner or the U.S. risks provoking stronger propogandist actions or other gray zone actions.

The solution set which addresses the majority of these stipulations leverages technology but is focused on the structure of institutions and frameworks rather than the technology itself. Politicizing information warfare threats against the U.S. only encourages and incentivizes Russian efforts. If their goal is to undermine our institutions and relationships, we only confirm the effectiveness of their methods with our parochial political treatment of the problem. Washington must speak in no uncertain terms of the value which we place in our security relationships, of the value of democracy, and that we view these Russian activities as unacceptable.

Bibliography

Anker, Andrew. "Launching New Trust Indicators From the Trust Project for News on Facebook." *Facebook Media*, Nov. 16, 2017, https://media.fb.com/2017/11/16/launching-new-trust-indicators-from-the-trust-project-for-news-on-facebook/

Apuzzo, Matt, and Sharon LaFraniere. "13 Russians Indicted as Mueller Reveals Effort to Aid Trump Campaign." *The New York Times*, February 16, 2018, sec. Politics. https://www.nytimes.com/2018/02/16/us/politics/russians-indicted-mueller-election-interference.html.

"Assessing Russian Activities and Intentions in Recent US Elections." Accessed January 7, 2018. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Buchko, Steven. "Blockchain's Fight Against Fake News." CoinCentral, March 26, 2018. https://coincentral.com/blockchains-fight-against-fake-news/.

Cadwalladr, Carole, and Emma Graham-Harrison. "Cambridge Analytica: Links to Moscow Oil Firm and St Petersburg University." *The Guardian*, March 17, 2018, sec. News. http://www.theguardian.com/news/2018/mar/17/cambridge-academic-trawling-facebook-had-links-to-russian-university.

Chaffetz, Hon. Jason. "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation." Committee on Oversight and Government Reform U.S. House of Representatives 114th Congress, September 7, 2016. https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf.

Chen, Adrian. "The Agency." *The New York Times*, June 2, 2015, sec. Magazine. https://www.nytimes.com/2015/06/07/magazine/the-agency.html.

Confessore, Nicholas. "New York Attorney General to Investigate Firm That Sells Fake Followers." *The New York Times*, January 27, 2018, sec. Technology. https://www.nytimes.com/2018/01/27/technology/schneiderman-social-media-bots.html.

"Detect and Track Political Bots on Twitter." Botcheck.me. Accessed March 3, 2018. https://botcheck.me/.

"French Foreign Legion Recruitment." French Foreign Legion Recruitment, March 2, 2018. http://en.legion-recrute.com/.

Frenkel, Sheera, and Daisuke Wakabayashi. "After Florida School Shooting, Russian 'Bot' Army Pounced." *The New York Times*, February 19, 2018, sec. Technology. https://www.nytimes.com/2018/02/19/technology/russian-bots-school-shooting.html.

"Frequently Asked Questions – The Trust Project." Accessed February 1, 2018. https://thetrustproject.org/faq/.

Fung, Brian. “Equifax’s Massive 2017 Data Breach Keeps Getting Worse.” *Washington Post*, March 1, 2018, sec. The Switch. https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/equifax-keeps-finding-millions-more-people-who-were-affected-by-its-massive-data-breach/.

Granville, Kevin. “Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens.” *The New York Times*, March 19, 2018, sec. Technology. https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

Griffith, Erin. “Pro-Gun Russian Bots Flood Twitter After Parkland Shooting.” WIRED, February 15, 2018. https://www.wired.com/story/pro-gun-russian-bots-flood-twitter-after-parkland-shooting/.

“Hamilton 68: Tracking Putin’s Propaganda Push... To America - About.” Hamilton 68. Accessed February 16, 2018. http://dashboard.securingdemocracy.org/about.

Hart (et al.), Hon. Gary. “International Security Advisory Board: Report on Gray Zone Conflict.” U.S. Department of State, January 3, 2017. http://www.state.gov/t/avc/isab/266650.htm.

Heickero, Roland. “Emerging Cyber Threats and. Russian Views on Information.” *Swedish Defence Research Agency*, 2017. http://www.highseclabs.com/data/foir2970.pdf.

Hinshaw, Drew, and Philip Heijmans. “Pro-Moscow Candidate Pulls Ahead in Czech First-Round Vote.” *Wall Street Journal*, January 13, 2018, sec. World. https://www.wsj.com/articles/czech-election-highlights-allure-of-russia-for-eastern-europe-1515758994.

“Joint Publication 3-13: Information Operations,” November 27, 2012.

Joyal, Paul M. “Cyber Threats and Russian Information Warfare.” *Jewish Policy Center* (blog), Winter 2016. https://www.jewishpolicycenter.org/2015/12/31/russia-information-warfare/.

Kapusta, Philip. “The Gray Zone.” U.S. SOCOM, September 9, 2015. https://info.publicintelligence.net/USSOCOM-GrayZones.pdf.

Kennedy, John F. “Remarks at West Point to the Graduating Class of the U.S. Military Academy.” The American Presidency Project, June 6, 1962. http://www.presidency.ucsb.edu/ws/index.php?pid=8695.

Kirk, Kira. “What Is VK and Why Should You Care?” Echosec, August 25, 2017. https://www.echosec.net/what-is-vk-and-why-should-you-care/.

Komonov, Maksim. “100 Million Russians Use Social Media Every Day.” *Practical Ecommerce* (blog), November 2, 2017. https://www.practicalecommerce.com/100-million-russians-use-social-media-every-day.

Krishnan, Armin. *Military Neuroscience and the Coming Age of Neurowarfare*. Emerging Technologies, Ethics and International Affairs. New York: Routledge, Taylor & Francis Group, 2017.

Lalic, Zoran. “A Deep Dive into Blockchain and Bitcoin.” *Insecure Magazine*, A deep dive into blockchain and Bitcoin, no. 57 (March 2018): 39–52.

“Launching New Trust Indicators From the Trust Project for News on Facebook | Facebook Media.” Accessed February 1, 2018. https://media.fb.com/2017/11/16/launching-new-trust-indicators-from-the-trust-project-for-news-on-facebook/.

Leetaru, Kalev. “The Scope of FBIS and BBC Open-Source Media Coverage, 1979–2008 (U).” *Studies in Intelligence* Vol. 54, no. No. 1 (March 2010). https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/volume-54-number-1/PDFs-Vol.-54-No.1/U-%20Studies%2054no1-FBIS-BBC-Coverage-Web.pdf.

Lo, Bobo. “An Accident Waiting to Happen: Trump, Putin and the US–Russia Relationship,” October 25, 2017. https://www.lowyinstitute.org/publications/accident-waiting-happen-trump-putin-and-us-russia-relationship.

“Machine Translation - Microsoft Translator.” Accessed May 7, 2018. https://www.microsoft.com/en-us/translator/mt.aspx.

Miller, Greg, Ellen Nakashima, and Adam Entous. “Obama’s Secret Struggle to Punish Russia for Putin’s Election Assault.” Washington Post, June 23, 2017. https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/.

“National Security Strategy of the United States of America.” Accessed January 7, 2018. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

O’Neil, Cathy. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. First edition. New York: Crown, 2016.

Priest, Dana, and Michael Birnbaum. “Europe Has Been Working to Expose Russian Meddling for Years.” *Washington Post*, June 25, 2017, sec. Europe. https://www.washingtonpost.com/world/europe/europe-has-been-working-to-expose-russian-meddling-for-years/2017/06/25/e42dcece-4a09-11e7-9669-250d0b15f83b_story.html.

“Records of the United States Information Agency (RG 306).” National Archives, August 15, 2016. https://www.archives.gov/research/foreign-policy/related-records/rg-306.

Reveron, Derek S., ed. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington, DC: Georgetown University Press, 2012.

Riddel, J. Niles. “Remarks by J. Niles Riddel, Foreign Broadcast Information Service.” Federation of American Scientists, December 2, 1992. https://fas.org/irp/fbis/riddel.html.

Rotella, Sebastian. “Russia’s Shadow-War in a Wary Europe.” ProPublica, April 4, 2017. https://www.propublica.org/article/russias-shadow-war-in-a-wary-europe.

“Russian Disinformation Distorts American and European Democracy - Turning Politics up to 11.” Accessed February 25, 2018. https://www.economist.com/news/briefing/21737297-mueller-indictment-reveals-some-kremlins-tactics-russian-disinformation-distorts.

Samet, Joshua S., " The United States Must Respond to Russian Perception Operations or Risk Losing Legitimacy Domestically and Internationally." Paper Submitted to U.S. Naval War College, National Security Affairs Department, on 7 February 2018

Solon, Olivia. “How Syria’s White Helmets Became Victims of an Online Propaganda Machine.” *The Guardian*, December 18, 2017, sec. World news. http://www.theguardian.com/world/2017/dec/18/syria-white-helmets-conspiracy-theories.

“The Fog of Wars.” *The Economist*, October 22, 2016. https://www.economist.com/news/special-report/21708880-adventures-abroad-boost-public-support-home-fog-wars.

“Un statut particulier.” Accessed March 3, 2018. test.

Underwood, Corinna. “Automated Journalism - AI Applications at New York Times, Reuters, and Other Media Giants -.” TechEmergence, June 22, 2017. https://www.techemergence.com/automated-journalism-applications/.

“Userfeeds Protocol Whitepaper [Draft].” Accessed May 15, 2018. https://userfeeds.io/Userfeeds_Protocol_Whitepaper_[Draft].pdf.

Varol, Onur, Emilio Ferrara, Clayton A. Davis, Filippo Menczer, and Alessandro Flammini. “Online Human-Bot Interactions: Detection, Estimation, and Characterization.” Center for Complex Networks and Systems Research, Indiana University, Bloomington, US and Information Sciences Institute, University of Southern California, Marina del Rey, CA, US, March 2017. https://arxiv.org/pdf/1703.03107.pdf.

“Vkontakte Wins an Appeals Lawsuit against Third-Party Data Mining.” Meduza. Accessed May 6, 2018. https://meduza.io/en/news/2018/01/30/vkontakte-wins-an-appeals-lawsuit-against-third-party-data-mining.

Walt, Stephen M. “Why Alliances Endure or Collapse.” *Survival* 39, no. 1 (Spring 1997): 156–79.