Countering Russian Meddling in US Political Processes

James P. Farwell
©2018 James P. Farwell

ABSTRACT: This article introduces a "team-of-teams" approach for countering Russian information operations such as those associated with democratic processes.

In early 2018, the Justice Department Special Counsel indicted 13 individuals and several companies associated with the St. Petersburg-based Internet Research Agency LLC. The parties allegedly interfered in US political processes as part of a Russian scheme to create chaos, inflame emotions, and polarize a divided public.[1] The effort also sought to discredit Hillary Clinton, whom President Vladimir Putin expected to win the Oval Office.[2]

The Special Counsel charged the accused with stealing identities, using PayPal to transfer money and to purchase Facebook ads, and falsely claiming to be US activists who contacted Donald Trump's campaign. The United States also said the accused made illegal campaign expenditures, failed to register as foreign agents, used false statements to obtain visas, and committed wire fraud. The most notable accusations involved organizing phony rallies, mounting a massive social media campaign to influence behavior, and paying Americans to carry out their objectives. It bears noting that many Western commentators presume that Putin directed this action. In our system, however, guilt must be proven beyond a reasonable doubt. Likewise, George Beebe, the respected former head of the Central Intelligence Agency's Russia analysis, stated the Internet Research Agency may have conducted this activity independently, without Putin's involvement.[3]

The Kremlin's strategy is to spread chaos for strategic effect, in order, as Peter B. Doran and Donald N. Jensen declared, "to confuse, distract, and disrupt."[4] Three premises underlie this strategy. First, an authoritarian regime can conduct cohesive information warfare or cyber warfare. Second, the regime can cope better with chaos, and thus advance its agenda. Third, weakening other nations strengthens the regime's power at home. While the United States views national security as protecting the nation, Putin sees it as ensuring his political survival.

Stopping Russian meddling requires an approach capable of developing strategic appreciation, forging and implementing a strategy,

Mr. James P. Farwell, an associate fellow in the King's Centre for Strategic Communication, Department of War Studies, Kings College, University of London and a nonresident senior fellow at the Middle East Institute, serves as a domestic and international political consultant. He has advised the US Special Operations Command and the US Strategic Command.

1 *United States v Internet Research Agency LLC et al.*, Criminal No. 1:18-CR-00032-DLF (2018), US District Court for the District of Columbia.

2 Michael Isikoff and David Corn, *Russian Roulette* (New York: Twelve, 2018).

3 George Beebe, "Here is What Trump Should Do about the Poisoning of a Former Russian Spy," *National Interest*, March 15, 2018.

4 Peter B. Doran and Donald N. Jensen, "Putin's Strategy of Chaos," *American Interest*, March 1, 2018.

and anticipating effects and consequences. First, the best *mechanism* to forge and implement strategy must be established. The "team-of-teams" concept that General Stanley McChrystal used in Iraq seems optimal, especially when the team is fully empowered to act through the National Security Council. Since national security is at stake, military leadership with bipartisan congressional oversight seems ideal for building trust and credibility. Once established, the United States should employ *active defense* to discredit and to delegitimize Russian actions. America then should engage in a *strategic offense* to "extract a cost from Putin that outweighs the benefits" and to persuade him to shift his efforts from US politics to shoring up his own.[5]

Russian experts interviewed for this commentary emphasized the importance of framing any national security plan in the context of the Kremlin, not Russia or Putin.[6] Given Putin's unpredictable, distrustful nature, attacking him personally could escalate matters. Characterizing Russia's actions as Kremlin activity makes the point with fewer downsides.

Team of Teams

A team-of-teams approach can leverage the unique resources and authorities commanded by the US presidency to forge and implement strategy. The public spokesperson for such a team should be a military professional such as Admiral Michael S. Rogers, the commander of US Cyber Command and director of National Security, or General Joseph Dunford, chairman of the Joint Chiefs of Staff.[7] The team should include nonpartisan and bipartisan national security experts with extensive knowledge of the political aspects of the team's efforts.

Such a diverse team would communicate collaboration and integrity to audiences who need to believe our nation's leaders are speaking the truth in today's polarized political environment. This combined effort would also balance the political polarity, often magnified by mass media, to seize and to maintain the critical moral high ground invaluable to information warfare. Audience trust is critical to enabling the government to articulate a credible rationale that explains what it is doing, why it is taking an action, and how the action will affect target audiences.

The team of teams is a proven concept. McChrystal employed a sophisticated one to fight al-Qaeda, and US political campaigns employ a simpler one. President Ronald Reagan applied the concept to counter Soviet active measures and to win public support for deployment of intermediate nuclear weapons in Europe. Ambassador Brian E. Carlson explains, "The cardinal principle of a team-of-teams approach recognizes that strategic leadership must flow from the White House."[8]

---

5 Dell L. Daily (retired lieutenant general, US Army; retired ambassador; former coordinator for counterterrorism for the Department of State), interview by author, March 13, 2018 (emphasis added).

6 Experts included Donald N. Jensen, chief of information warfare for the Center for European Policy Analysis and former diplomat who served in Moscow; George Beebe, former director of the Central Intelligence Agency's Russia analysis; King Mallory, senior researcher at the RAND Corporation; Jeffrey Starr, former deputy assistant Secretary of Defense for Russia, Ukraine, and Eurasia; and others.

7 This idea emerged in discussions with Colonel Jeremiah R. Monk (US Air Force, and deputy director, NATO Centre of Excellence Defense against Terrorism in Ankara, Turkey).

8 Brian E. Carlson (former ambassador and former chief liaison with the Department of Defense on strategic communication and public diplomacy for the State Department), interview by author, February 13, 2018.

The cooperative nature of a team of teams counters the tendency of a bureaucracy to strangle planning and action.[9] A *Harvard Business Review* survey of 7,000 readers recently found bureaucracy creates bloat, friction, insularity, disempowerment, risk aversion, inertia, and politicking. Bureaucracy also devours time on preparing reports, complying with internal requests, and burying employees beneath multiple management layers.[10] A team of teams can avoid such inefficiencies.

McChrystal's business partner, Chris Fussell, observes that Putin understands how to exploit information-age threats: "Putin leverages many of the same factors that allowed al-Qaeda to become an exceptionally destabilizing force."[11] Fussell notes Russia employs diverse strategies, operations, and tactics in carrying out its propaganda activities. No single solution or entity, can defeat either. A wide range of parties, many working as small teams, is required.

Fussell states, "Small teams do their best work when they communicate faster and more effectively than the problems they face." The challenge is to scale that approach to the enterprise level. In Iraq, "thousands of personnel, from a wide range of organizations, resynchronized on a very aggressive cadence in order to move faster than al-Qaeda, which could rewrite the rules as they saw fit on any given day." Although al-Qaeda moved quickly, McChrystal's team moved faster, a pivotal capability that allowed the general to tailor his approach to Iraq. Fussell also notes that the communication structure moved quickly:

> Resynchronizing for 90 minutes every 24 hours. . . . the sessions would include thousands of participants around the globe. More important than the cadence or methodology of these forums was the end state they aimed to achieve. The intent of each session was to reestablish a shared consciousness between those involved, that is, a common understanding of what the problem looked like in the moment, and what new intelligence was most critical to the next phase of decision-making.[12]

A team of teams can involve fewer participants than the thousands McChrystal engaged against al-Qaeda. The approach is what matters. A team of teams could help identify Moscow's real-time stories, narratives, themes, and messages, recognizing the active channels, voices, and key influencers. The team could facilitate integrated, cohesive, and coherent messaging and countermessaging strategies. With this information, the collaborative organization would be able to maintain situational awareness to support effective operations and tactics. Team members could quickly coordinate resources across the military, government agencies, domestic organizations, and partner nations.

The team's activities would include identifying media outlets or social media sites associated with Russian intelligence; conducting target audience analysis; and holding accountable journalists who

---

9 Stanley A. McChrystal, *Team of Teams: New Rules of Engagement for a Complex World* (New York: Portfolio, 2015); Chris Fussell, *One Mission: How Leaders Build a Team of Teams* with C. W. Goodyear (New York: Portfolio, 2017); and Stanley A. McChrystal, *My Share of the Task* (New York: Portfolio, 2013).

10 Gary Hamel and Michele Zanini, "What We Learned about Bureaucracy from 7,000 HBR Readers," *Harvard Business Review*, August 10, 2017; and Gary Hamel, "Why Bureaucracy Must Die," *Fortune*, March 26, 2014.

11 Chris Fussell (managing partner and chief growth officer at McChrystal Group), interview by author, September 29, 2017.

12 Fussell, interview.

sell their services to Russian news channels. This information would support Justice Department action to force such parties to register under the Foreign Agents Registration Act. In this manner, a team of teams can integrate all elements of national power, including the military, counterintelligence, the intelligence community, the State Department, and the Justice Department.

The military's experience in employing the team-of-teams approach in contemporary situations makes it suitable for organizing and administering the team. Military expertise in cyber and electronic warfare techniques will also prove vital to detecting Russian internet channels and mitigating their impact on American interests. Assessing options for leveraging pressure points such as Ukraine also requires an appreciation for military strategy.

Interagency Cohesion

No single US government department or agency would prove as effective as a team of teams. None possesses the required authorities, resources, or political influence.

Department of State. The mission of the Department of State's Global Engagement Center was broadened in 2017 to fight "foreign propaganda and disinformation" directed against US national security interests and "proactively promote fact-based narratives" that support United States allies and interests.[13] The center's last permanent chief, Michael D. Lumpkin, earned praise and the current staff is smart and hard-working. Former Deputy Assistant Secretary of Defense for Russia, Ukraine and Central Asia, Jeffrey Star, summarizes one inherent challenge the institution faces: "No single department or agency possesses the clout, expertise, or resources to make things happen across the US government on the scale needed to counter Russian disinformation."[14] The center's authority and flexibility to sole-source contracts for required subject matter expertise, an essential requirement for forging and executing fast-moving campaign strategy, is unclear. Some State Department officials indicate proposals submitted to the Global Engagement Center may take as much as a year to process. Putting it mildly, this timeframe is too long.[15]

Department of Defense. The Defense Department brings unique strategic and organizational expertise that a team of teams requires. But countering the Kremlin's information warfare demands a strong national strategy led by the president. In this conflict paradigm, information warfare, not kinetic operations, will prove decisive. The military's resources and leadership are best deployed in this type of engagement through a team of teams.[16] The Defense Department's role, which includes employing cybertools and addressing escalatory issues, is broad. Our military possesses unique capabilities to conduct essential human factors analysis essential to pressuring key actors who

13 National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, 130 Stat. 2001 (2016).

14 Jeffrey Starr, interview by author, January 30, 2018.

15 Interviews by author.

16 Robert J. Giesler (former chief of Strategy and Plans in the Strategic Capabilities Office, Secretary of Defense and former director of Information Operations and Strategic Studies), interview by author, February 15, 2018.

can influence Putin. Theater security cooperation activities offer a viable counterpropaganda platform. The military must also lead North Atlantic Treaty Organization (NATO) cooperation important to other global security efforts.

Interagency Fusion Cell. The minority staff of the Senate Committee on Foreign Relations has advocated for a fusion cell, modeled on the approach used by the National Counterterrorism Center, to counter Russian influence operations.[17] The most challenging aspect of this approach involves relying exclusively on government expertise. The pace and complexity of information warfare requires a wide range of outside experts—many with unconventional skills—who can be hired on a sole-source basis. Beebe cautions such cells establish another bureaucracy as departments and agencies rarely "send their top-tier talent to these teams. And once the representatives arrive, typically their priority is to put the interests of their parent organization ahead of the fusion cell."[18] As Carlson adds, such task forces have previously "crashed and crumbled on the sharp rocks of each agency's distinct mission, budget, congressional mandate, regulations, procedures, and self-image" with little success in achieving their purpose.[19]

The intelligence community should support the team of teams. But in contrast to the covert nature of intelligence activities, efforts of the team of teams should be overt. Persuading the Kremlin to back down requires transparency. The public needs to understand what the Kremlin is doing. Putin needs to understand the consequences of Kremlin actions. A team of teams can capitalize on the strengths of all elements of national power to achieve its objectives and leverage the power of the presidency to maximize them.

Employ Active Defense

The notion of active defense embraces many options. The team of teams should focus on understanding foreign propaganda efforts, recognizing the individual and organizational agents that influence American interests, involving private industry in disseminating accurate and transparent information, and improving legislative accoutrements by increasing enforcement of established laws and expanding restrictions on employing bots.

Understand Propaganda

The military's cybercapability is ideal for identifying the communication channels that are creating propaganda and for achieving the reach, penetration, and impact of the narratives, themes, and messages. Target audience analysis can identify what stories, narratives, themes, and messages are circulating—*and the language in which they are articulated.* The analysis can reveal how messages resonate with different audiences through opinion research, such as focus groups and surveys, and behavioral research that identifies how language affects audiences intellectually and emotionally. Target audience analysis also integrates

17 *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security, Prepared for the Senate Committee on Foreign Relations*, S. Prt. 115-21, 115th Cong 155 (January 10, 2018).

18 George Beebe, interview by author, February 10, 2018.

19 Carlson, interview.

opinion research with intelligence sources and uses information gained from grassroots and grasstops engagement.[20] This information can be shared with US audiences to help them understand the nature of communications originating with parties promoting foreign interests. Measures of attitudes and opinions gained from this information will also allow the team of teams to forge winning narratives, themes, and messages and to allocate resources. The military's experience in target audience analysis makes it the most appropriate leader for this effort.

Recognizing Agents

Most Americans lack awareness of the many media outlets, such as RT and RIA Global LLC (*Sputnik*), that are linked to Russian intelligence. English language shows—such as *News with Ed Schulz*, *Larry King Now*, *America's Lawyer* with Mike Papantonio, and *Going Underground*—and the employment of American journalists provide foreign news outlets with false legitimacy as independent news organizations.[21] Can anyone imagine the American journalist Edward R. Murrow selling his services to German propagandist Joseph Goebbels like Larry King has to RT?

Walter Isaacson, former managing editor of *Time* and chief executive officer of CNN, argues efforts to discourage individuals from contributing to such propaganda must be pursued cautiously with a goal of achieving resiliency: "I would not favor imposing official or legal sanctions on American citizens working for such organizations, because it could set a dangerous precedent that restricts free speech. . . . But if someone is shilling for an organization you believe is harmful, you have an absolute right to call them out for it, and I think that we should."[22]

The United States could, for example, prohibit business activity under the Countering America's Adversaries through Sanctions Act similar to the Treasury Department and the Office of Foreign Assets Control prohibitions against Iran and Libya.[23] The team of teams can identify the best approach for holding US citizens accountable for associations that support and legitimize Russian propaganda while forging resilience.

Role of Industry

Industry groups should be discouraged from treating foreign propaganda operations as legitimate organizations. For example, when the International Academy of Television Arts and Sciences considers RT for Emmy Awards in news and current affairs, the American people might begin to associate the media channel communicating Russian intelligence messages as a trustworthy source.[24] By drawing upon industry and legislative expertise, the team of teams could appropriately

---

20 James P. Farwell and Darby J. Arakelian, "Using Information in Contemporary War," *Parameters* 46, no. 3 (Autumn 2016): 76–86. Political consultants refer to opinion leaders as "grasstops."

21 "Shows," RT, accessed April 26, 2018, https://www.rt.com/shows/.

22 Walter Isaacson, interview by author, February 26, 2018.

23 Countering America's Adversaries through Sanctions Act, Pub. L. No. 115-44 (2017); "Iran Sanctions," US Department of the Treasury, April 16, 2018, https://www.treasury.gov/resource-center/sanctions/Programs/Pages/iran.aspx; and "Libya Sanctions," US Department of the Treasury, March 6, 2018.

24 "RT Becomes First Ever Russian TV Channel To Get Emmy News Nomination," RT, January 1, 2000, https://www.rt.com/about-us/press-releases/rt-becomes-first-russian-tv-channel-emmy-news-nomination/.

develop sanctions that offer an actionable strategy and determine laws or amendments to existing laws to achieve this goal.[25]

Improving Legislation

Enforcing current laws. The decision to require Sputnik International, RT, and *RIA Global LLC* to register under the Foreign Agents Registration Act, which covers agents "seeking economic or political advantage for their clients," was significant.[26] The act covers "foreign political parties, a person or organization outside the United States, except U.S. citizens, and any entity organized under the laws of a foreign country or having its principal place of business in a foreign country."[27] The statute excludes news or press agencies if ownership is held by at least 80 percent US citizens and the organization is not directed, supervised, controlled, subsidized, or financed by any foreign principals. Using the Foreign Agents Registration Act for all sites associated with foreign intelligence agencies would force Moscow to label their "informational materials" with a conspicuous disclosure of the agents acting for a foreign principal.[28] Exposing this truth will help discredit the manipulative communications.

Expanding restrictions. A study by Oxford University's Samuel C. Woolley and Philip N. Howard examined "the use of algorithms, automation, and human curation to purposefully distribute misleading information over social media networks," in contexts such as the use of bots during the 2016 US elections. Their research examined 17 million tweets from 1,798,127 unique users and concluded "false news reports . . . can in many cases be considered to be a form of computational propaganda. Bots are often key tools in propelling this disinformation across sites like Twitter, Facebook, Reddit, and beyond."[29] The study concluded that bots challenge the integrity of democratic political processes because they "are easily programmable . . . can be deployed by just about anyone with preliminary coding knowledge. . . . [and can be used] to create an illusion of popularity around fringe issues or political candidates."[30]

Some researchers have concluded bots are "capable of massively distributing propaganda in social and online media" and can be "partly responsible for recent election results."[31] Bots enable operators to flood voter perceptions with false or misleading assertions that can overwhelm

---

25 For one example of flawed legislation that could benefit from the team of teams, see the Countering America's Adversaries through Sanctions Act. Peter Baker and Sophia Kishkovsky, "Trump Signs Russian Sanctions into Law, With Caveats," *New York Times*, August 2, 2017.

26 Foreign Agents Registration Act of 1938, 22 U.S.C. §611 et seq (2011); Nathan Layne, "U.S.-Based Russian News Outlet Registers as Foreign Agent," Reuters, February 17, 2018, https://www.reuters.com/article/us-usa-trump-russia-propaganda/u-s-based-russian-news-outlet-registers-as-foreign-agent-idUSKCN1G201H; and "Criminal Resource Manual: 2062. Foreign Agents Registration Act Enforcement," Offices of the United States Attorneys, https://www.justice.gov/usam/criminal-resource-manual-2062-foreign-agents-registration-act-enforcement.

27 "General FARA Frequently Asked Questions," US Department of Justice, August 21, 2017, https://www.fara.gov/fara-faq.html#1.

28 22 U.S.C. 611(d).

29 Samuel C. Woolley and Philip N. Howard, *Computational Propaganda Worldwide: Executive Summary*, working paper 2017.11 (Oxford: University of Oxford, 2017), 3, 5, 8, 9.

30 Douglas Guilbeault and Samuel Woolley, "How Twitter Bots Are Shaping the Election," *Atlantic*, November 1, 2016.

31 Christian Grimme et al., "Social Bots: Human-like by Means of Human Control?," *Big Data* 5, no. 4 (December 1, 2017): 279, doi:10.1089/big.2017.0044.

the capacity of humans to respond. Aided by the coming era of artificial intelligence, the dangers posed by bots are going to escalate. In *The Madcom Future*, a highly recommended publication, Foreign Service Officer Matt Chessen articulates the dangers of a dystopian social media environment that this technology poses.[32]

The Constitution guarantees US citizens freedom of speech. But that right does not extend to robots. In fact, algorithmic assessments and automated messages generated through artificial intelligence, especially when such "speech" influences elections, should not be protected. To prevent the use of such technology from manipulating US citizens, social media platforms should be required to authenticate whether a human is not only responsible for managing each account but is also communicating from it. The authenticity of human communications becomes more important as the ability of artificial intelligence to create artificial realities using avatars on social media platforms increases the challenges of countering fake news and disinformation.

The Strategic Offensive

Offensive tactics and operations should be strategically layered and executed, which requires military appreciation and leadership. Persuading Putin to back down is *Realpolitik* that requires understanding his perception of the strategic situation and his motivations. Many commentators believe the Kremlin instigated the election meddling. But the Russian experts interviewed for this article agreed with reports that the Kremlin felt it merely responded to its perception of US aggression such as the bombing of Belgrade in 1999, retaining Muammar Gadhafi in Libya, and meddling in Russian elections.[33] The experts agree Hillary Clinton's criticism of Putin infuriated him and served as a key motivator for the Kremlin's meddling in the US election of 2016.[34]

Realistically, offensive actions may best be aimed at establishing, in Beebe's words, a "rules of the road" by which all sides refrain from meddling in election infrastructure in Russia, the United States, and other Western nations.[35] Establishing that framework will require strategic military input as well as an evaluation of political and diplomatic considerations. The task is daunting but doable. Strategy needs to be thought through carefully and executed to account for Putin's emotional, unpredictable nature.

---

32 Matt Chessen, *The Madcom Future: How Artificial Intelligence Will Enhance Computational Propaganda, Reprogram Human Culture, and Threaten Democracy . . . And What Can Be Done about It*, (Washington, DC: Atlantic Council, 2017).

33 Evan Osnos, David Remnick, and Joshua Yaffa, "Trump, Putin and the Cold War," *New Yorker*, March 6, 2017; Arkady Ostrovsky, *The Invention of Russia* (New York: Penguin, 2015); Mikhail Zygar, *All the Kremlin's Men: Inside the Court of Vladimir Putin* (New York: PublicAffairs, 2016); Andreĭ Soldatov and Irina Borogan, *The Red Web: The Kremlin's Wars on the Internet* (New York: PublicAffairs, 2015); "Statement on Addition of NDI to Russian 'Undesirable Organizations' List," NDI, March 10, 2016, https://www.ndi.org/Statement-Russian-Undesirable-Organizations-List; and "Russia Adds International Republican Institute to Growing List of 'Undesirable Organizations,'" International Republican Institute, August 18, 2016, http://www.iri.org/resource/russia-adds-international-republican-institute-growing-list-%E2%80%9Cundesirable-organizations%E2%80%9D.

34 Will Kirby, " 'Revenge' Vladimir Putin 'Interfered in the US Election To Get Back at Hillary Clinton,' " *Express* (London), December 12, 2016; and Isikoff and Corn, *Russian Roulette*.

35 George Beebe, interview by author, March 23, 2018.

Increase Political Pressure

The team of teams could coordinate a human factors analysis through the Department of Defense to identify key state and state-proxy influentials whose agendas Putin spends much time balancing. By understanding the recipients of Putin's selective repression and manipulation, which includes arrests and feeding interpersonal animosity among Russia's leaders, strategists can target individuals such as Dmitry Rogozin, who was recently promoted from presiding over Russia's growing military-industrial complex, and Yevgeny Prigozhin, dubbed "Putin's Chef," who runs the indicted internet research company, to exert pressure.[36] These individuals and other influentials could add pressure for Putin to back off US election interference.[37] While this article refrains from itemizing all the legal tools available to make the lives of influential Russian's difficult, plenty of options exist: assigning an unwanted label such as "criminal" and conducting hours of Customs and Border Protection questioning are but two inconvenient pressures. There are any number of ways to make the daily lives of Russian dignitaries more difficult, and irritate them to the point that they complain to Putin.

If more intense efforts become necessary, financial sanctions, cybertools, and weaponized social media can also play havoc in their personal lives. In this situation, Putin may find attending to the whining influentials preferable to meddling in foreign elections.[38] A less optimal tactic involves imposing complete sanctions at a single stroke. Layered tactics will enable the team of teams to develop an effective strategy to gradually increase the pressure and clearly communicate the tactics will stop when Putin does. Putin might not yield if the demand is to change his policies on Ukraine; however, he may well prove responsive to demands about our elections.

Apply Distractive Measures

In addition to creating a political environment that forces Putin to focus his attention closer to home, the same types of weaponized social and broadcast media employed against the United States can be used to discredit and to delegitimize Putin's leadership in Russia. That strategy would also require him to respond to domestic issues. Russians are aware of the concentration of wealth and power in their country. Yet a 24/7 direct broadcast satellite news service could expose corruption, nepotism, and incompetence that Russians already suspect. America's driving of that narrative will aggravate Putin.[39]

Putin lacks the total control once exerted by Joseph Stalin. He does not control events. That renders his regime politically brittle. We could use social and broadcast media to attack the history the Kremlin invokes to justify its actions. That history includes the myth that World War II was a patriotic war that united Russians and that it was won without

36 The United States has already instituted some sanctions against notable Russians. "Общегражданский проект «Список Путина»" (The All-Citizens Project: Putin's List), Forum Free Russia, December 5, 2017, https://www.forumfreerussia.org/main/2017-12-05/obshhegrazhdanskij-proekt-sostavlyaem-spisok-putina-2/.

37 Mikhail Zygar, *All the Kremlin's Men*; and interviews with Mallory, Jensen, and Beebe.

38 Donald P. Jensen, interview by author, February 27, 2018.

39 King Mallory, interview by author, February 16, 2018.

allied help.[40] A reminder that Stalin sent returning prisoners of war to labor camps, sponsored mass deportations of Chechens and others, and acted as a despotic tyrant would challenge Russians' perceptions of the state. Changing fixed attitudes and beliefs that a target audience holds is challenging. But Putin roots his policies in the myth, which he cannot afford to lose.

These actions require military leadership to support the target audience analysis, provide strategic appreciation, and develop the story, narrative, theme, and message. Given Putin's tendency toward emotional and unpredictable reactions, clear communications to the Kremlin about what and why actions are being taken must be conveyed by credible communicators to avert avoidable escalation. The military can also conduct beneficial military-to-military back-channel communications with the Kremlin, which provides another reason for a servicemember to be the public face of the team of teams.

Employ Cybertools

The capability to use cybertools against critical infrastructure offers strategic and tactic opportunities. The *Washington Post* reported Obama "authorized planting cyberweapons in Russia's infrastructure, the digital equivalent of bombs that could be detonated if the United States found itself in an escalating exchange with Moscow."[41] Reportedly, he left the decision on whether to use the capability to President Trump. The complex nature of this decision, as well as the magnitude of intended and unintended consequences arising from employing malware, mandate the president seek expert advice on potential scenarios and effects before approving cyberaction.

A properly configured team of teams would possess this expertise. The knowledge would enable the team to understand the intricacies associated with precise targeting and to address relevant concepts. Some experts on the team will recognize the intended and unintended political consequences of using cybertools. The team must use this information to guide the team's development of clear explanations and recommendations for the National Security Council and the president. Experts involved with Stuxnet, for example, could explain the importance of differentiating "between the propagator, or boost-phase code that disseminates the program, and the actual payload code that creates the physical effect on a target (the distinction between the gift wrapping and the gift)" to protect the global network while affecting the intended target.[42]

The broad perspective developed by the team of teams can limit situations identified by Herbert Lin in which factors such as "poorly designed malware and inadequate intelligence can cause unintended collateral damage." Incidents occurring because of these factors may appear "deliberate rather than accidental . . . thereby setting the stage for escalation." Lin explains, "Using cybertools to retaliate against Russian interference in our political process may be appropriate and

40 Donald P. Jensen, interview by author, February 23, 2018.

41 Greg Miller, Ellen Nakashima, and Adam Entous, "Obama's Secret Struggle to Punish Russia for Putin's Election Assault," *Washington Post*, June 23, 2017; and Isikoff and Corn, *Russian Roulette*.

42 James P. Farwell and Rafal Rohozinski, "The New Reality of Cyber War," *Survival* 54, no. 4 (August-September 2012): 108, doi:10.1080/00396338.2012.709391.

useful, but only if the United States is willing and able to tolerate a Russian counterresponse."[43] One tactic that merits close consideration is neutralizing known Russian bots that interfere in our elections such as those used by the Internet Research Agency.

Stabilize International Relations

Putin has staked his leadership credibility on his actions in Ukraine, which creates a strategic pressure point. Competing schools of thought argue how best to exploit this potential. Experts such as Jensen believe Russia will never accept Ukrainian neutrality between Russia and the West; they argue for bolstering Ukrainian security and economic resilience. Experts such as Beebe are more optimistic about stabilizing these relationships and foresee a neutrality agreement that excludes the possibility of Ukraine joining NATO.

The strategy debate for Ukraine lies in another venue. Yet the pressure point of Ukrainian-Russian relations should be leveraged. Furthermore, the strategy should also include locating a military information support operations team in our embassy in Kiev.

Conclusion

Nikki Halley, US ambassador to the United Nations, has characterized Russia's meddling as "warfare."[44] The White House possesses the clout to counter Russia's disinformation activity. Employing a team-of-teams approach will improve the president's understanding of the available options. Tough decisions may be necessary—for example, altering voter rolls or election outcomes may justify attacking Russian critical infrastructure. Such action mandates communicating the consequences to the Kremlin clearly, privately, and precedently.[45]

America's communication during information and cyber warfare must build and maintain trust in the truth, articulate a credible rationale for the necessary action, and claim the moral high ground for it. The credibility of the US military argues for using it as the face of national security matters. Working with a team of teams, military contacts with the Russian military will enable constructive engagement to avert avoidable or accidental escalation. The military's expertise in psychological and influential operations, cybertools, electronic warfare, and assessing Russian capabilities and intentions align with the pivotal role for forcing the Kremlin to stop meddling in US election processes.

An empowered team of teams can forge and execute active defense to discredit and to delegitimize Russian action in the United States. The team can compel Putin to shift his focus away from US politics to his affairs at home. But we need to take action before the escalation cycle becomes irreversible.

---

43 Herbert Lin, interview by the author, February 19, 2018.

44 Maegan Vazquez, "Nikki Haley: Russian Cyberinterference into US Elections Is 'Warfare,'" CNN, October 19, 2017, https://www.cnn.com/2017/10/19/politics/nikki-haley-russia-warfare/index.html.

45 Annabelle Dickson and Laurens Cerulus, "British Cyber Option to Punish Russia Prompts Fear of 'Electronic War,'" *Politico*, March 13, 2018.