A Duty to Warn

How to Help America Fight Back against Russian Disinformation

Maj William Giannetti, USAFR

An unclassified Intelligence Community Assessment released in January 2017 by the National Intelligence Council (NIC) claimed Russia interfered with the US presidential election. This interference operation was directed by President Vladimir Putin and carried out by Russia's civilian and military intelligence services: the Federal Security Service and the Main Intelligence Directorate. The NIC report followed a US intelligence community investigation into e-mails stolen from the Democratic National Committee in 2016. The e-mails contained sensitive communications between leaders of the Democratic Party, senior staff members, and the party's candidate for president, which once exposed, served to embarrass and discredit them all. The NIC assessed that these e-mails were stolen by Russian hackers associated with the aforementioned organizations. The hackers deliberately handed the e-mails to WikiLeaks, an antigovernment secrecy group, who promptly released all their compromising details to the news media. The Russian stunt was part of a plan to "denigrate" the Democratic Party candidate to sway American public opinion away from her and toward her Republican opponent.[1]

The assessment—if true—details one of the most elaborate cyber operations ever committed by a nation-state against the United States and its political process. To denigrate the candidate, online agitators—known as trolls—published disinformation that claimed that she suffered from various, fictitious maladies and poor mental health. English-speaking Russian state media outlets, like *Russia Today* (*RT*) and the online *Sputnik*, ran stories that excoriated the candidate while casting her opponent as the target of unfair media coverage by traditional news outlets that were "subservient to a corrupt political establishment."[2] Up to this point, hostile cyber operations have arguably been synonymous with spear-phishing, which ensnares unsuspecting victims into disclosing access codes, or with the denial of service attacks that can disrupt or degrade computing systems. Nonetheless, if executed skillfully by their perpetrators, cyber operators can also manipulate information—that most intangible, but precious commodity that Winn Schwartau presciently wrote about more than 20 years ago—to misinform, confuse, and disorient an entire electorate.[3]

What can the Air Force do about a sophisticated attack of this nature that uses cyberspace as a delivery vehicle? It has a cyberspace operations doctrine that mainly focuses on protecting web-based government and military information technology infrastructure from catastrophic attacks and suggests common-sense approaches to defense of same, such as maintaining firewalls or installing antivirus software to protect against intrusions.[4] But, how can we "go on the offensive" and protect the nation from disinformation campaigns like the one outlined in the IC's report? It may not take computer logic or code; rather, it will probably take a concerted, combined effort undertaken by law enforcement, intelligence, and cyber professionals alike to combat the problem. European countries, such as the Czech Republic, are preparing to defend themselves by examining web content for disinformation and building its public's awareness to it.[5] Undeniably, protecting government and military computing systems is important work; if it is in jeopardy from a threat borne out of cyberspace, then the Air Force's premier cyberspace warriors have a duty to warn of its imminent collapse. So, do we have a duty to warn when disinformation hits our shores and threatens to subvert or derail our political process?

The Beginning of a New Era

In 2005, the Air Force avowed itself to fly, fight, and win in air, space, and cyberspace. This was a bold statement because it marked the first time any service—anywhere—named cyberspace as a domain to be conquered in a presumably wartime situation. That same year, the World Wide Web had evolved to its current state: Web 2.0. Gone were the days of the 1990s when websites and their content were static and cumbersome. In today's Web 2.0 world, everything—all content—is dynamic and user-defined. It almost goes without saying that this was a revolution in terms of how we communicate with each other, from an individual level, all the way to the highest corridors of power at the national level. One year later, a fascinating thing occurred. In 2006, technicians at the Idaho National Laboratory conducted a test on an industrial, diesel generator with the purpose of hacking into its control systems and disabling it from afar. The technicians established a base of operations 100 miles away and exploited vulnerability in the machine's control code.[6] Their interference caused the 1–ton machine's power converters to cycle on and off in such rapid succession that it began to shudder, overheat, and eventually self-destruct in a cloud of smoke.[7] The powerful images, when they were broadcast on television, were a preview of the mayhem that might await us. What this example also demonstrated was that, in a sense, the machines that provide us with power and light were almost as connected as human beings were becoming on an individual level. It showed that a generator could be disabled using remotely deployed malicious code and that our worst fears about the vulnerability of our critical infrastructure in this new age of interconnectivity could be realized. This new reality became most palpable to the tiny Baltic nation of Estonia in 2007.

That year Estonia—at 95 percent connectivity—was reputedly the world's most wired nation. In April, it was decided that a Soviet-era memorial to the Russian soldiers who died during the Second World War would be moved from the center of its

capitol city Tallinn to the outskirts of the city. Russian-speaking Estonians took to the streets that month in a massive protest. What followed was even more concerning: a rush of distributed denial of service attacks using a sophisticated botnet of an estimated 85,000 computers caused an abrupt slowdown of the nation's communications and banking infrastructure.

Estonia withstood the attacks through the Russian Victory Day holiday that May—which commemorated the Soviet's victory over Nazi Germany—when 58 websites were brought down at once, and services from its largest financial institution were unavailable for 90 minutes. The outages continued until late May and, although the political, social, and economic damage was noticeable, the physical damage was "minor."[8] Naturally, the source of the attacks could not be localized and, while all fingers pointed toward Russia, Moscow completely disavowed any involvement in the attacks. Initially, evidence brought by the Estonian authorities pointed the origination of the attacks to Russian Internet protocol (IP) addresses. The Estonians retracted this statement later as the evidence was determined to be inconclusive.

Other attacks of this sort would follow. In December 2016 in the Ivano–Frankivsk region of Ukraine, a power plant technician reportedly witnessed his terminal's cursor leap to life and, in a very deliberate fashion, begin to shut down the breakers of his substation, plunging approximately 230,000 people into darkness. The outage lasted between one and six hours and, fortunately, Ukrainian power companies harmed by the incident had enough data logged by their firewalls to reconstruct how the breach occurred. The preparatory phases of the attack began with a classic, mid-1990's style, spear-phishing campaign that targeted power plant workers using a Microsoft Word document enclosed in an e-mail. To download the document and the malware inside, a user would have to click on a prompt, which would enable macros inside it. Once enabled, a short script in Visual Basic would command the computer to seek out and record log-in credentials. After the attackers gathered enough user name and password information, they accessed the power company's Windows domain controllers, where more user names and passwords were kept, until they found credentials for workers who used virtual private networks to log in remotely to the power companies Supervisory Control and Data Acquisition network. From there, the hackers remotely took control of the Ukrainian power station virtually unopposed.[9] The virus was still as effective in 2016 as it was 20 years ago, although its code and means of dissemination lacked for originality.[10]

Cyber Warfare or Political Warfare?

Looking simply at these incidents alone, one could conclude that what happens in faraway Estonia or Ukraine could conceivably happen here at home, so the Air Force's focus on protecting itself and the Department of Defense (DOD) network infrastructure from intrusions certainly seems justifiable enough. It has an implicit interest in protecting publicly networked systems external to it as well because doing so enables "force deployment, training, transportation, and normal operations."[11] Routine updates to antimalware software should be conducted so all the latest vul-

nerabilities are patched, and the passwords to control systems must be strong enough to mitigate the possibility they might be easily cracked.

But when we are talking about DOD networks or public networks, there are almost no safeguards to prevent the spread of disinformation, especially the likes of which the NIC published in glaring detail. The discussion about enacting said safeguards has turned inevitably to questions like, "Was our election hacked?" or "Was this the cyber Pearl Harbor that people have envisioned for so many years?"[12] The answer to both questions is, emphatically, "no." The truth of the matter is what the Russians unleashed is not cyber war—at least not according to our classic understanding of it as the brief case studies above illustrate. Rather, this is political warfare, the kind that uses cyberspace as a medium to deliver what Russian intelligence officers might call *disinformatsiya* and *kompramat*, or politically damaging information.[13] On a semifrequent basis, the Department of Homeland Security (DHS) publishes bulletins regarding the spread of malicious code and responsibly tells citizens and their businesses how to defend themselves against it. What made the ICA so special, however, was it was the first report of its kind to alert the public about Russia's disinformation campaign, which was designed to force an outcome ostensibly in its favor.

For that matter, the United States is no stranger to foreign powers' disinformation operations. One of the modern era's first, and arguably most successful, attack was perpetrated, not by Russia, but by the United Kingdom's British Security Coordination (BSC). In her book *The Irregulars*, Jennet Conant tells the story of the BSC, which ran its spy ring out of Washington, DC and Rockefeller Center in New York City. The BSC's general purpose at the time was to snap the nation out of its "America First" mentality, to spur a change in its isolationist policy of nonintervention during the Second World War, and cause it to throw its material support behind Europe. In an ingeniously deceptive plan, the BSC's chief, a Canadian citizen named William Stephenson, led the production of a forged German map depicting safe houses in southern Cuba, where equipment caches were located, radio sites to signal German U-boats, and a postwar plan to carve up North Atlantic territories into Nazi protectorates. Ivar Brice, a British agent who worked for the BSC at the time, said Stephenson tipped off his Federal Bureau of Investigation (FBI) contacts of the map's existence and the safe house where it could be found. The map would sound the alarm in America that the Nazi threat was closer to her shores than previously thought. "Were a German map of this kind be discovered or captured from enemy hands," he wrote, "and publicized. . . among the "America Firsters" with their belief that America could get along with Hitler, what a commotion would be caused."[14]

The forgery was found by the FBI and delivered to Stephenson, who passed it to the head of the Office of Strategic Services, Gen William Donovan, who, in turn, delivered it to President Franklin D. Roosevelt. In reaction, the president took to the airwaves, and in March 1941 he delivered a radio address to the nation revealing that he had in his possession a "secret map" which outlined the contrived Nazi plan and included what he called "our great lifeline" to the Pacific—the Panama Canal. "That map, my friends," said the president, "makes clear the Nazi design, not only against South America, but against the United States as well." President Roosevelt

went on to promise America would now "pull its oar" in Europe's struggle against fascism and Germany.[15]

In the 1960s and 1970s, before the Internet age, Russian propaganda and disinformation made its way into books published by authors who were paid to take part in then-Committee for State Security (KGB) operations in the United States called "active measures." The KGB funded and used Communist agents like Italian-born Carl Aldo Marzani, whose publishing houses, the Liberty Book Club and the Prometheus Book Club, were among the first to shed doubt on the Warren Commission's finding that Lee Harvey Oswald acted alone during President John F. Kennedy's assassination. Writers in Marzani's employ, like Joachim Josten, who were funded by grants from the Communist Party of the Soviet Union, wrote books that accused Oswald of being "an FBI agent provocateur with a CIA [Central Intelligence Agency] background."[16] Doing so, according to KGB archivist and dissident Vasili Mitrokhin, established two of the most enduring falsehoods in Kennedy assassination lore: that there was a government conspiracy to kill the president, and the CIA was involved.

Of all the agents who brought ignominy to the CIA's doorstep in the 1970s, none was more damaging that Philip Agee. Agee was the Edward Snowden of his day, a man who wrote three books that detailed CIA clandestine operations around the world and exposed an estimated 2,000 CIA officers. Agee, according to Mitrokhin, was summarily fired from the CIA in 1968 because of his poor financial habits and excessive drinking. In his disgust, he first attempted to defect with a trove of classified documents to the KGB resident office in Mexico City. The officer in charge of the Mexico City office at the time was Oleg Kalugin.[17] Kalugin, sensing a trap, turned Agee away. Still, Agee found a willing audience eventually in Cuba, whose intelligence service shared the stolen intelligence with the Russians anyway. The KGB, when Agee's first memoir, *Inside the Company*, was published in 1975, bore no compunction about taking credit for helping the author and the Cubans prepare it. It is unclear, though, how much preparation or work the KGB actually put into Agee's book, but the would-be defector did acknowledge later that the Communist Party of Cuba, and the Cuban intelligence service, "gave important encouragement at a time when I doubted I would be able to find the additional information I needed." The CIA, in its *Studies in Intelligence* journal, according to Mitrokhin, admitted Agee's work was a "severe body blow" to the agency.[18]

The book met with critical acclaim around the world while Agee lived in exile in London. Soon, he faced deportation and, as his reputation as a whistle-blower grew, prominent politicians from England and the United States (including one former US attorney general) came out in defense of his actions. Mitrokhin recounts in Agee's KGB file, support campaigns for his *cause celebre* were initiated in nine nations. He was eventually forced to leave London for Holland in 1977, but the KGB was "jubilant" at the chaos the entire affair had caused, and the embarrassment the CIA suffered.[19]

Making the Russian Connection

At this point, after examining some of the technical intricacies within Russia's cyber operations and methods of political warfare, we now turn to a brief exploration

into Moscow's motivations. What is its purpose? There are a couple of theories. One theory is that the intrusion upon the Democratic Party was retribution for embarrassing economic sanctions placed on Moscow, its defense industries, and financial institutions following human rights abuses it committed during its combined campaign with Iran against Islamic State militants in Syria. Economic sanctions were also levied against Russia following the invasion of Ukraine and annexation of Crimea. These things, in its view, were part of a deliberate US-led campaign to bring disgrace upon the Russian military which would, therefore, turn public opinion against it.[20] Sanctions also push Russia toward pariah status by degrading its prestige in world politics and, more importantly, the international arms market. They devalue its weapons manufacturing businesses, and potentially undercut the profits of the oligarchs who run them.

Another vastly interesting theory is President Putin commands a government with intelligence services comprised of disruptive forces who thrive on chaos. In a mid-December interview, shortly after the ICA's release, Gleb Pavlovsky, a former advisor of the Russian president, remarked: "Of course the Kremlin likes the fact of such an atmosphere of chaos. Because we are traders of chaos. We sell it, and the more chaos there is in the world, the better it is for the Kremlin."[21] Indeed, this theme of chaos harkens back to the Agee case. Chaos, in Moscow's view, causes Russia's adversaries to react hysterically and make seemingly unfounded allegations that, according to Putin, "distract the attention of the American people from the substance of what the hackers had put out."[22] This statement, oddly enough, presumes that the stolen e-mails, in all their scurrilousness, might somehow shed light on American political deliberations that would otherwise be hidden from public view, and that the former KGB officer is some sort of free media advocate. In any case, the United States, according to his rationale, is deflecting the blame for its political process' shortcomings—and the source of its scandals—upon Russia. Alternately, allegations of election tampering have the opposite effect of making President Putin appear to be an altogether cunning and provocative operator who drives his enemies to distraction as they attempt to find the source of the intrusions.

Time to Try Something Different

In any event, now that we know Russia's motivations and the purpose of its actions, how do we defend against them? Leaders of the US IC—former director of National Intelligence James Clapper and Adm Mike Rogers, commander of US Cyber Command—previewed the findings of the ICA during Senate testimony on 5 January 2017. Director Clapper said the IC ought to undertake a counterpropaganda initiative to prevent any future meddling in the United States' electoral process. One recommendation he made was to revive the US Information Agency (USIA), a Cold War–era organization that for a time led our public diplomacy abroad, and credibly communicated the country's values, official positions, and policies to counter Communist disinformation.[23] During questioning, senators asked why the USIA's charter had not been renewed yet. Admiral Rogers said, "I do not think we have come yet to a full recognition of the idea that we are going to have to try to do something fun-

damentally different."[24] The admiral, who is also director of the National Security Agency, added, "I think we still continue to try to do some of the same traditional things we've done and expecting to do the same thing over and over again, yet achieve a different result."[25] By the early 1990s, the USIA had outlived its usefulness and fell into disrepute after the fall of the Soviet Union. The organization's material lost its persuasiveness and no longer seemed relevant, given the dissolution of its ideological reason for being.

Confronting and combatting Russian disinformation in the United States will not necessarily take hauling out agencies past, or will it take an entirely novel approach. In fact, our cyberspace operations doctrine is premised upon a tried and true guiding principle: the best offense is a good defense. Former Air Force Chief of Staff Gen Norton A. Schwartz recommended common-sense measures for USAF and DOD systems in November 2011 that could conceivably apply to public and private sector networks which are also vulnerable to cyberattack. To deny an adversary the freedom of maneuverability in cyberspace, a defender must bar access to sensitive information and systems. The import of General Schwartz's words is that one must build an awareness of malicious code and the malign actors who seek to find ways to implant it into our computers at work and at home. Keeping unauthorized software and peripheral devices—like thumb drives—away from our computers is one means people could use to prevent the spread of viruses, worms, or botnets. Using protective antivirus software is another. Ignoring e-mails that are not signed digitally, or that contain attachments with executable macros and hyperlinks from unverifiable sources, is a more common but effective means of a sound cyber defense.[26] These measures seem commonplace today, but they were built upon the experiences and hard lessons learned about the sources of intrusions since 2005.

When it comes to protecting Air Force, DOD, or public networks from the pernicious effects of disinformation, the solutions are neither technical, nor clear. A case study from the Czech Republic, however, is instructive because it provides a viable, minimally invasive, and thus reasonable alternative. There, a small unit of 15 social media analysts actively monitor Twitter, Facebook, *Sputnik*, and pro-Russia Czech language news sites inhabited by online agitators who purvey disinformation. The group, which is headed by Benedikt Vangeli, was established to ferret out so-called "fake news" that flummoxed Czechs by harshly disparaging pro-NATO or European Union politicians before their parliamentary elections in October. Taking to Twitter, the unit will simply flag questionable news sources and alert the public of their inauthenticity. "We just tweet them to the public as false reports," Vangeli says. "That's how we fight back. We don't take them down. We don't censor." Similar groups of this sort have been set up in Germany and Finland, and could reasonably be established in the United States as well.[27]

At its heart, Vangeli's approach of a prudent public awareness campaign, which—like General Schwartz's recommendations—is based on common sense and a duty to simply warn the public. Now, a cynic might say that the military (the Air Force in this case) should not tell the public it works for what to read or what to think. Doing so in the United States, where freedom of speech is guaranteed in its Constitution, would mean its citizenry watching all their Orwellian nightmares about government intervention into matters of free speech and thought come true. Preempting

harmful messages online might also impinge upon citizens' expectations of privacy and their freedom of choice as they browse the Internet, or potentially constitute an illegal search if the proper legal authorities are not in place first. Air Force instructions do, however, state that subject to DOD regulations, Airmen can cooperate with and assist law enforcement during investigations that protect against "clandestine activities" against the United States (like the Russian plot recounted here), and protect the department's "employees, information, property, or facilities."[28] Presuming that they are already monitoring the web for disinformation, it is entirely possible that federal law enforcement agencies who are endowed with the proper statutory authorities will have to identify anomalies first, then notify their military counterparts to summon their expertise in winnowing down the exact source of the offending information down to the IP address. The pooling of resources, nevertheless, will be critical, and the stakes are high. The negative consequences for failing to warn the public about disinformation will be grave; the nation's faith in its governing institutions could be irreparably damaged, and worse yet, its collective consciousness perpetually poisoned.

Since 9/11, our government and military have learned the values of collaboration and cooperation—that our collective manpower and know-how will triumph over the parochialism that stifled information sharing and innovation before that terrible day. In short, law enforcement organizations, like the FBI, which has sole authority to conduct counterintelligence operations in the United States, and the Air Force Office of Special Investigations (AFOSI), should partner and lead a joint counterdisinformation task force. This task force could be small like the Czechs' or emulate the FBI's larger joint terrorism task forces (JTTF). With more than 100 across the country, JTTFs are the nation's premier mechanism for counterterrorism collaboration with a variety of local, state, and federal law enforcement agencies.[29]

The AFOSI could represent the DOD's counterintelligence equities, while the DHS Computer Emergency Readiness Team can employ its know-how with identifying the sources of cyber disinformation, the subtleties of their coding, and the networks of individuals who propagate it.[30] Undoubtedly, fighting back against disinformation will require a partnership with the country's private sector. The FBI is the leader of InfraGard: a consortium of more than 30,000 subject matter experts in a variety of fields, such as computer engineering, technology, and security. Finally, with a proper mandate from the Air Force's director of intelligence, our Airmen in the cyber and intelligence career fields can come off the bench and become active participants in a new endeavor that could very well unmask future Russian propagandists, expose the truth behind their activities, and protect our nation against political warfare's corrosive effect. ✪

Notes

1. National Intelligence Council, *Assessing Russian Activities and Intentions in Recent U.S. Elections* (Washington, DC: Intelligence Community Assessment, 6 January 2017), 2, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

2. Ibid., National Intelligence Council, 4.

3. Winn Schwartau, *Information Warfare–Cyberterrorism: Protecting Your Personal Security in the Electronic Age* (New York: Thunder's Mouth Press, 1996, 2nd ed.), 35, 638.

4. Curtis E. LeMay Center for Doctrine Development and Education, "Annex 3-12 *Cyberspace Operations*," 30 November 2011, 5, https://doctrine.af.mil/DTM/dtmcyberspaceops.htm. The Air Force in this passage of its doctrine implicitly acknowledges that is has a vested interest in protecting publicly networked systems because they enable things like "force deployment, training, transportation, and normal operations."

5. Anthony Faiola, "Czech Republic Enlists Unit to Combat Disinformation," *The Washington Post* (23 January 2017), A1, A10.

6. Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013), 46.

7. For footage of the test, see: https://www.youtube.com/watch?v=fJyWngDco3g.

8. Ibid., 6.

9. Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired.com*, 3 March 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

10. Schwartau wrote that the Word for Windows Macro Virus was "the most prevalent virus around" in June 1996. At that time, he said it was "spreading at least 10 times faster than any other virus in history," and ibid., Schwartau, 21.

11. Curtis E. LeMay Center for Doctrine Development and Education, "Annex 3-12 Cyberspace Operations," 30 November 2011, 5, https://doctrine.af.mil/DTM/dtmcyberspaceops.htm.

12. In his book *Information Warfare,* Schwartau references his 1991 testimony to Congress. He warned the legislature of a future "electronic Pearl Harbor" because the government writ large was ill prepared to defend the country's increasingly interlinked computers against a catastrophic attack (see Schwartau, 43). See, also, Ralph Peters, "Washington Ignores Cyberattack Threats, Putting Us All at Peril," *Wired.com*, 23 August 2007, https://www.wired.com/2007/08/ff-estonia-america/amp/.

13. Peter B. Zwack, "Russia," in *Charting a Course: Strategic Choices for a New Administration*, ed., R.D. Hooker Jr., 238, Washington, DC: National Defense University, December 2016, http://ndupress.ndu.edu/Portals/68/Documents/Books/charting-a-course/charting-a-course.pdf?ver=2016-12-08-154300-120. See, also: "A Russian Word Americans Need to Know: Kompramat," *NPR*, 11 January 2017, http://www.npr.org/sections/parallels/2017/01/11/509305088/a-russian-word-americans-need-to-know-kompromat/.

14. Jennet Conant, *The Irregulars* (New York: Simon and Schuster, 2008), 94.

15. Ibid., Conant, 95.

16. Christopher Andrew and Vasili Mitrokhin, *The Mitrokhin Archive and the Secret History of the KGB* (New York: Basic Books, 2009), 226–27.

17. Oleg Kalugin retired from the KGB as a major general after 32 years of service. Today, he serves on the International Spy Museum's Advisory Board of Directors in Washington, DC. See: https://www.spymuseum.org/about/leadership/board-of-directors/.

18. Ibid., Andrew and Mitrokhin, 231.

19. Ibid., 232.

20. David Filipov, "Putin Uses the Soviet Defeat of Hitler to Show Why Russia Needs Him Today," *Washington Post*, 8 May 2017, https://www.washingtonpost.com/world/europe/putin-is-using-the-soviet-defeat-of-hitler-to-show-why-russia-needs-him-today/2017/05/07/1c390338-2e9e-11e7-a335-fa0ae1940305_story.html?utm_term=.10033df265ff.

21. David Filipov, "'Chaos' Theory Is Working for Putin," *Washington Post*, 15 December 2017, A-1, A-12.

22. Ibid., Filipov.

23. Statement of James Clapper, director of national intelligence, US Senate Committee on Armed Services in Senate, "Hearing to Receive Testimony on Foreign Cyber Threats to the United States," 5 January 2017, 112.

24. Statement of Admiral Mike Rogers, director of the National Security Agency, US Senate Committee on Armed Services in Senate, "Hearing to Receive Testimony on Foreign Cyber Threats to the United States," 5 January 2017, 112.

25. Ibid., Admiral Rogers' testimony.

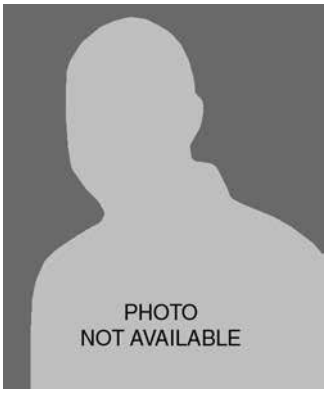
26. Curtis E. LeMay Center for Doctrine Development and Education, "Annex 3-12 Cyberspace Operations, Appendix A: CSAF Remarks on Cyberspace," 41, (30 November 2011) from: https://doctrine.af.mil/DTM/dtmcyberspaceops.htm.

27. Ibid., Faiola, A10.

28. US Air Force Instruction 14-104, "Oversight of Intelligence Activities," *www.epublishing.af.mil.*, 5 November 2014. See, also: Department of Defense (DOD) Regulation 5240 1.R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons*, and DOD Instruction 3025.21, *Defense Support of Civilian Law Enforcement Agencies*.

29. Former FBI Director Robert Muller oversaw the post-9/11 expansion of joint terrorism task forces (JTTF) to every field office in the nation. As of 2014, 71 JTTFs were created after the terrorist attacks. See, also, Bruce Hoffman, Edwin Meese, Tim Roemer et al., "The FBI: Protecting the Homeland in the 21st Century," FBI National Press Office (25 March 2015), https://www.fbi.gov/news/pressrel/press-releases/the-fbi-releases-final-report-of-the-9-11-review-commission.

30. The FBI and DHS, in cooperation with the Department of Homeland Security's Computer Emergency Readiness Team, released an unclassified report in December 2016 which broke down how Russia's intelligence services using a focused spear phishing campaign to gain access to senior Democratic Party staff members e-mails in spring 2015 and summer 2016. The report, which dubbed the Russians advanced persistent threats 28 and 29, said the actors "masqueraded as third parties, hiding behind false online personas designed to cause the victim to misattribute the source of the attack." Unlike the ICA, the FBI–DHS report does not go so far as to directly blame Russia president Vladimir Putin for the intrusion. See, also, the FBI–DHS Joint Analysis Report, *GRIZZLY STEPPE—Russian Malicious Cyber Activity* (Washington DC: 29 December 2016), https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.



Maj William Giannetti, USAFR

Major Giannetti (MS, St. Joseph's University) is an Air Force reservist assigned to the joint staff at the Pentagon, Washington, DC. His 20-year career spans time as a civil servant, Philadelphia police officer, and Department of Defense analyst. He was a staff member of the 9/11 Review Commission, which examined how the Federal Bureau of Investigation implemented the original commission's recommendations. Major Giannetti also served two tours in Afghanistan.