Prepared Statement of GEN (Ret) Keith B. Alexander*
on
Disinformation: A Primer in Russian Active Measures and Influence Campaigns
before the
United States Senate Select Committee on Intelligence

March 30, 2017

Chairman Burr, Vice Chairman Warner, Members of the Committee: thank you for inviting me to discuss "*Disinformation: A Primer in Russian Active Measures and Influence Campaigns*" with you today, and specifically, how the ongoing revolution on how we create and communicate information, particularly in cyberspace, makes it easier for nations like Russia to undertake successful active measures campaigns, particularly in the realm of information operations, including overt and covert propaganda and disinformation efforts, in furtherance of national political goals. I would like to briefly touch on some of the things we ought do, working together, to combat such activities and to protect our nation—our government, our private sector, and our people—from these and other threats in cyberspace. In particular, I believe it is critical that our public and private sectors work more closely together. This Committee and the relevant agencies in the Executive Branch can play a key role in helping make that happen.

I want to thank both Chairman Burr and Vice Chairman Warner for your bipartisanship and for making cybersecurity and counterintelligence top priorities for this committee, including the Chairman's work on the Cybersecurity Information Sharing Act and Vice Chairman Warner's efforts with Senate Cybersecurity Caucus and on the Digital Security Commission Act. It is also worth noting that this committee has held more than 10 hearings and briefings over the last two years to examine the scale and scope of Russian activities,[1] and that as early as June 2016, this committee sought to require the establishment of a committee "[t]o counter active measures by Russia to exert covert influence over peoples and governments."[2]

Active measures have been utilized by Russia since the 1920s, perhaps most famously during the Cold War. Retired KGB Maj. Gen. Oleg Kalugin describes these "subversion" activities as "the heart and soul of the Soviet intelligence" that were specifically designed to "weaken the West, to drive wedges in the Western community alliances of all sorts, particularly

* Gen. (ret.) Keith B. Alexander is the former Director, National Security Agency and the Founding Commander, United States Cyber Command. Currently, he is the President and CEO of IronNet Cybersecurity and recently completed service as a member of the President's Commission on Enhancing National Cybersecurity.

[1] *See* Federal News Service, *Transcript: Full Committee Hearing on Russian Intelligence Activities*, Senate Select Committee on Intelligence (Jan. 10, 2017).

[2] *See* Intelligence Authorization Act for Fiscal Year 2017 § 501, *available online at* <https://www.intelligence.senate.gov/legislation/intelligence-authorization-act-fiscal-year-2017-reported-june-6-2016>.

NATO, [and] to sow discord among allies."[3] According to Kalugin, this "worldwide campaign…conducted and manipulated by the KGB," included "all sorts of forgeries and faked material…targeted at politicians, the academic community, [and the] public at large."[4] Likewise, Vasili Mitrokhin, a former senior KGB archivist, described the bulk of KGB active measures as "'influence operations' designed to discredit the [United States]...[through] disinformation fabricated by…the active measures branch of the [KGB]."[5] During the Cold War, these activities included efforts to undermine the FBI, the State Department, and civil rights leaders, as well as efforts to incite racial violence and hatred, including through the dissemination of false information about private organizations, individuals, and the government via false publications and materials misattributed to particular individuals or organizations, among other things.[6]

In many ways, this description of historic Soviet active measures is strikingly similar to what this committee described last year as Russian covert influence active measures, including the "[e]stablishment or funding of [] front group[s]…[c]overt broadcasting…[m]edia manipulation…[and] [d]isinformation and forgeries, funding agents of influence, incitement, and offensive counterintelligence, assassinations, or terrorist acts."[7] Director Clapper likewise indicated that "Moscow's influence campaign blended covert intelligence operations with overt efforts by Russian government agencies, state funded media, third party intermediaries and paid social media users" and that "Moscow's behavior reflects Russia's more aggressive cyber posture in recent years, which poses a major threat to U.S. military, diplomatic, commercial and critical infrastructure networks….[and] demonstrate[s] a significant escalation in directness, level of activity, and scope of effort compared to previous operations."[8]

At the same time, it is certainly worth noting that aggressive efforts to collect intelligence on our elections are not new – indeed, ODNI has made clear that in 2008, the "foreign intelligence services…track[ed the] election cycle like no other" and "targeted the campaigns…[m]et with campaign contacts and staff[,] [u]sed human source networks for policy insights, [e]xploited technology to get otherwise sensitive data, [and] [e]ngaged in perception management to influence policy."[9] Indeed, Russia use of *kompromat* (compromising information), *maskirovka* (military deception), and proxy assets to disseminate propaganda (both official and unofficial) is likewise not new.

---

[3] *See* CNN, *Inside the KGB: An Interview with Maj. Gen. Oleg Kalugin* (Jan. 1998), *available online* at <https://web.archive.org/web/20070206020316/http:/www.cnn.com/SPECIALS/cold.war/episodes/21/interviews/kalugin/>.

[4] *Id*.

[5] *Id*.

[6] *See, e.g.*, *id*. at 234-39.

[7] *See* Intelligence Authorization Act for Fiscal Year 2017 § 501.

[8] *Id*.

[9] *See* ODNI, *Unlocking the Secrets: How to Use the Intelligence Community* (Dec. 10, 2008), at 12-13, available online at <https://icontherecord.tumblr.com/post/143906537893/new-freedom-of-information-act-request-documents>.

Efforts like these are empowered by the modern era of technology and, in particular, by the scale and scope of information traversing our networks. The amount of information circulating the globe via IP networks will reach 2.3 zettabytes by 2020, the "equivalent of all the movies ever made [] cross[ing] the global Internet every 2 minutes."[10] And it will be transmitted over 26.3 billion networked devices, more than three IP-connected devices per person worldwide.[11] At the same time, according to Pew Research, "a majority of U.S. adults – 62% – get news on social media," and given the penetration of some of these services, message targeting can be broad in scale yet highly focused. For example, Pew estimates up to 44% of the general population in the United States gets some measure of its news on Facebook.[12] And given the continued development and rapid iteration of technology and Internet-enabled platforms, these trends are likely to continue and even accelerate.

While this might not seem particularly troubling at first blush, it is worth evaluating in the context of potential efforts to manipulate information. Back in the Cold War era, if the Soviet Union sought to manipulate information flow, it would have to do so principally through its own propaganda outlets or through active measures that would generate specific news: planting of leaflets, inciting of violence, creation of other false materials and narratives. But the news itself was hard to manipulate because it would have required actual control of the organs of media, which took long-term efforts to penetrate. Today, however, because the clear majority of the information on social media sites is uncurated and there is a rapid proliferation of information sources and as other sites that can reinforce information, there is an increasing likelihood that the information available to average consumers may be inaccurate (whether intentionally or otherwise) and may be more easily manipulable than in prior eras. It is likewise easier to generate "buzz" and "hype" about particular events or storylines (again, whether accurate or inaccurate) because of the speed at which news is conveyed amongst the population.

These efforts also take place in the context of larger cyber efforts by our peer competitors, including the ongoing, massive theft of intellectual property from American companies and the use of actual destructive attacks on both public and private sector entities in the United States and abroad.[13] The reality is that as a free society, we have many vulnerabilities and leave ourselves open to threats—including propaganda and disinformation attacks—that more authoritarian nations may be more capable of combatting by limiting access to resources or restricting the freedom of their people. And it is worth noting that our enemies today need not attack our government to have a substantive strategic effect on our nation. Attacking civilian or

---

[10] *See* Cisco, *The Zettabyte Era—Trends and Analysis* (June 2016) at 1, 4, *available online at* <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.pdf>

[11] *See Zettabyte Era*, n. 3 *supra* at 2.

[12] *Id*.

[13] These activities include destructive attacks against Saudi Aramco and Qatari RasGas in 2012, more recent attacks against the Saudi government, and destructive attacks conducted by nation-states against private institutions in the United States, including the Las Vegas Sands Corporation and Sony Corporation, not to mention massive disruptive attacks targeting American financial institutions. *See* Keith B. Alexander, *Prepared Statement on A Borderless Battle: Defending Against Cyber Threats*, U.S. House Committee on Homeland Security (March 22, 2017), at 2 & n. 1-3, available online at <http://docs house.gov/meetings/HM/HM00/20170322/105741/HHRG-115-HM00-Wstate-AlexanderK-20170322.pdf>.

economic targets, including through disinformation, may be a more effective approach in the modern era, particularly for asymmetric actors like terrorist groups. Moreover, as the number of nations that possess the capability to exploit and attack continues to grow, there is more of a chance that those with less of an incentive to act in line with appropriate state-to-state behavior will begin using cyber capabilities in a more aggressive way.

What all of this fundamentally means is that the future of warfare—including information operations—is here, and we need to structure and architect our nation to defend our country in cyberspace. Specifically, in my view, it is critical that as a nation, we fundamentally rethink how the government and the private sector relate to one another in cyberspace. We need to draw clear lines and make explicit certain responsibilities, capabilities, and authorities. And because the private sector controls the vast majority of the real estate in cyberspace, particularly when it comes to critical infrastructure and key resources,[14] there is no question that the government and private sector must collaborate. We need to recognize that neither the government nor the private sector can capably protect the systems and networks that our nation relies upon without extensive and close cooperation.

For the government to effectively work with the private sector to secure the nation in cyberspace, perhaps the single most important thing the government can do is to build real connectivity and interoperability with the private sector. This effort must be a two-way partnership between government and the private sector: the government can and must do more when it comes to partnering with the private sector, building trust, and sharing threat information—even highly classified threat information—at network speed, and in a form that can be actioned rapidly. Building out a cross-cutting information sharing capability allows the government and private sector to develop a common operating picture, analogous to the air traffic control picture. Just as the air traffic control picture ensures our aviation safety and synchronizes government and civil aviation, the cyber common operational picture can be used to synchronize a common cyber defense for our nation, drive decision-making, and enable rapid response across our entire national cyber infrastructure. In my view, if properly implement, this could prove a critical defensive capability for the nation.

While much remains to be done to fully put our nation on a path to real security in cyberspace, I am strongly hopeful for our future. With your leadership, Mr. Chairman, and that of the Vice Chairman, working together collaboratively across the aisle and with the White House and key players in the private sector, as well as other key committees in Congress, I think we can achieve some real successes in the near future.

[14] *See, e.g.*, Office of the Director of National Intelligence, Office of the Program Manager-Information Sharing Environment, *Critical Infrastructure and Key Resources*, available online at <https://www.ise.gov/mission-partners/critical-infrastructure-and-key-resources> ("The private sector owns and operates an estimated 85% of infrastructure and resources critical to our Nation's physical and economic security.").