INTELLIGENCE AND
NATIONAL SECURITY ALLIANCE

POSITION PAPER

May 2018

GETTING AHEAD OF FOREIGN INFLUENCE OPERATIONS

Distinguishing Messages from Malware

Prepared by
THE INSA CYBER COUNCIL

EXECUTIVE SUMMARY

Russia's extensive use of Facebook and Twitter to sow discord during the 2016 presidential campaign has made clear that both public and private sector cybersecurity programs are poorly equipped to identify foreign influence operations. Government agencies and corporations focus primarily on defending against cyber attacks that target their technical infrastructure, often at the expense of detecting cyber-based influence operations that seek to shape beliefs. By searching for malware that could damage their networks, they are missing malicious messages that damage our nation.

It is imperative that we differentiate between technical attacks *targeting* cyber infrastructure and influence operations *using* cyber infrastructure. The former penetrates networks to either steal information or produce malicious effects on a network. The latter employs cyber infrastructure to deliver political or sociological messages to produce a desired effect in the public discourse. By focusing on technical cyber attacks – which hold data at risk and undermine confidence in the ability to conduct business online – the U.S. government, the media, and the public typically miss signs of *influence* operations. Influence operations obscure truths, exacerbate rifts in the public discourse, and undermine the ability of public officials to conduct diplomacy and craft policy.

To defend against hostile messages as well as technical attacks, this paper will illustrate why both government agencies and private companies must:

- Differentiate between cyber attacks and influence operations;
- Encourage collaboration between information security officials who can see signs of an attack and foreign affairs experts who understand foreign adversaries' intentions;
- Promote engagement between government, industry, academia, and the media that enhances their collective ability to identify influence operations and to educate the public on their adverse impact; and
- Make use of artificial intelligence and machine learning (AI/ML) to identify malicious messages contained in the bits and bytes that cross an organization's cyber infrastructure.

INTRODUCTION

Cyber attacks targeting computer networks and other technical infrastructure typically garner widespread attention, as they impede organizations' operations and, in many cases, place sensitive public and private data at risk. Perhaps just as significantly, such attacks undermine public confidence in the Internet as a reliable platform for conducting business.

However, by focusing on technical cyber attacks, the U.S. government, the media, and the public typically miss signs of *influence* operations. Influence operations obscure truths, exacerbate rifts in the public discourse, and undermine the ability of our public officials to conduct diplomacy and to craft and execute policy.

Government agencies and corporations focus principally on defending against cyber-based attacks that target their technical infrastructure, often at the expense of cyber-based influence operations that seek to shape, undermine, or attack beliefs. The resulting myopia makes it easier for adversaries to influence American politics, policy, and society.

INFORMATION OPERATIONS, CYBER ATTACKS, AND INFLUENCE OPERATIONS

Before launching into any discussion, it is important to have an understanding of the lexicon.

The Defense Department defines **information operations** as "the integrated employment, during military operations, of information-related capabilities *in concert* with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own." The disruptive impact on an adversary's decision-making could be accomplished by harming the adversary's technical systems – for example, by obstructing the flow of information. However, the ultimate aim is not to affect information handling systems, but rather to diminish the quality of decisions. The goal is to lead an adversary to follow false or inaccurate streams of information (no matter how it is delivered) or to undermine an adversary's confidence in the accuracy of information. Russia's concept of **information warfare** is similar in this respect, in that it is designed, regardless of delivery method, to "steal, plant, interdict, manipulate, distort or destroy information," according to a NATO Defense College publication.[1]

The National Institute of Standards and Technology (NIST) defines a **cyber attack** as "an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information."[2] Cyber attacks designed to sabotage or compromise critical systems can contribute to information operations by disrupting the target's decision-making abilities.

> The goal [of information operations] is to lead an adversary to follow false or inaccurate streams of information or to undermine an adversary's confidence in the accuracy of information.

In an **influence operation,** information is weaponized or retooled as a mechanism for social engineering with intent to influence decision-making. For example, a publicly released diplomatic cable—whether real or fabricated—can embarrass a government by implicating it in nefarious or illegal activities. Allegations from unspecified sources, backed by "proof" of varying reliability, can convince many that a government is operating in a manner inconsistent with its stated policy goals. Rumors circulated on social media can gain prominence and credibility though mere repetition and move quickly into mainstream media.

Both technical cyber attacks and influence operations are forms of information operations. Influence operations operate on a sociological plane; they target groups or individuals with messages that appeal to the audiences' beliefs, prejudices, and world views with an expectation that the messages will influence or sway the audiences' opinions in ways favorable to the messenger. Influence operations rely on the most appropriate communications media for reaching the target audience; forms of dissemination have included rumor campaigns, printed materials such as pamphlets and leaflets, print journalism, national and international radio broadcasting, and, most recently, social media. Cyberspace is the perfect medium in which to conduct influence operations as it is anonymous, scalable, and global.

Ultimately, whether technical or sociological in nature, information operations target adversary decision-making by compromising either the technical systems that support decision-making processes or the content of the information used to make decisions.

"Cyberspace is the perfect medium in which to conduct influence operations as it is anonymous, scalable, and global.

REAL WORLD EXAMPLES: CONTEMPORARY RUSSIAN INFLUENCE OPERATIONS

It is often possible to attribute actions in cyberspace to a person or organization, though connecting the dots and producing high confidence attribution assessments remains a major challenge. Understanding the doctrine and strategy of major political adversaries and economic competitors can provide insight to help develop these assessments. Considering recent events, the case of Russia is illustrative.

Available literature makes clear that the Russian concept of information warfare is not limited to wartime activities; in fact, it spans the entire spectrum of peace, crisis, war, and post-war environments.[4] Russia realizes—as a matter of doctrine—that information warfare has both technical and psychological components. Furthermore, Russian strategy posits that the country is in a state of constant engagement, or confrontation, with its adversaries to influence the development and outcome of global political struggles. *Information confrontation* combines both defensive and offensive components and provides insight into how Russia orchestrates its largely state-controlled media and information infrastructure as an instrument of state policy.[5]

Both the U.S. Intelligence Community and technology companies like Facebook have reported that Russia's military intelligence agency, the Main Intelligence Agency of the General Staff of the Russian Armed Forces (GRU), uses cyber networks as a means for transporting and shaping information to achieve strategic objectives[6,7]. Russia's "active measures" campaigns deliver information, particularly disinformation and propaganda, to confuse and destabilize its adversaries. The messages the GRU delivers are not hidden in the bits and bytes of electronic communications; they are typically delivered and disseminated in plain sight, with only the originator of the messages being cloaked.

"The messages the GRU delivers are not hidden in the bits and bytes of electronic communications; they are typically delivered and disseminated in plain sight, with only the originator of the messages being cloaked.

Russian influence operations employ cutting-edge technology to advance Moscow's strategic goals of splitting the Euro-Atlantic alliance, sowing discord within the European Union, and creating havoc in Western public discourse. Official government news agencies, state-funded news services such as Russia Today (RT) and Sputnik News, third-party intermediaries, and a sizable cadre of paid social media provocateurs, or "trolls," reportedly work collaboratively to advance anti-American and anti-Western themes.[8] These outlets can also provide political cover for sensitive influence activities carried out by clandestine services.

Below are just a few recent examples of Russian influence operations designed to have strategic effects in the United States or regarding U.S. policy.

- In February 2014, a publicly disseminated audio recording of a phone call between a senior State Department official and the U.S. ambassador in Kiev proved highly embarrassing to the United States and frustrated U.S. diplomacy during a political crisis in Ukraine. While attention focused on the content of the conversation, few asked how such a sensitive communication could even be recorded, let alone "leaked" to the public. The recording was first released via Twitter and YouTube from unidentified Russian sources. The State Department was forced to concede that the endeavor demonstrated "pretty impressive tradecraft" and that "only a few countries have the capability needed" to execute such a complex operation combining intelligence collection and covertly directed communications.[9]
- In October 2017, Facebook informed a congressional committee that a Russian "troll farm" was behind the creation of fraudulent accounts whose divisive social and political postings reached 126 million people.[10] The political messages targeted American Facebook users – particularly in swing states like Michigan and Wisconsin – during the 2016 presidential campaign.[11] On Facebook, Twitter, and other social media sites, thousands of fake accounts that were carefully cultivated to appear authentic disseminated automated election-related postings. Such "bots" often sent links to newly created web sites that appeared to provide authentic news. As real social media users visited the web site and posted their own links to the bogus articles, the fake news acquired a semblance of mainstream legitimacy.[12]

- Almost a year after the tragic murder of Democratic National Committee (DNC) staffer Seth Rich in Washington, D.C., Russian media and social media bots repeated rumors that Rich was the source of leaked DNC emails which WikiLeaks – possibly with the encouragement of the Russian government – subsequently published.[13] This false narrative, disseminated widely through Internet news and information sites, deflects attention from the U.S. Intelligence Community's finding that Russian intelligence services were, in fact, responsible for the leaked emails.[14]

Russia's social media campaigns, in particular, highlight the notion that one cannot divine the intent of a message merely by examining bits and bytes. Many of the social media accounts posting messages appeared at first glance to be genuine. Only when the content of widely spread messages began to be seen as suspect were patterns identified that traced the postings back to fake accounts and bots linked to Russia.

BREAKING DOWN SILOS TO DEFEAT INFLUENCE OPERATIONS

One of the greatest challenges to identifying and understanding foreign information operations is that security officials and analysts – those who are best positioned to recognize an attack's means and content, respectively – operate in silos. The resulting myopia affects both government agencies and private companies.

> "Information systems security officers should receive sociological training to identify and evaluate the content of influence operations and techniques used for social engineering.

Information system security officers (ISSOs), including chief information security officers and chief risk officers, tend to focus on the technical aspects of electronic communications, not the content nor the intention behind it. The focus is on identifying and mitigating malware and other technical means of conducting a cyber attack. This approach may help ISSOs defend against a hacker exfiltrating or altering data on an organization's network while allowing information-based attacks to persist undetected.

Private companies, skilled at monitoring for and identifying malware, are unlikely to flag surreptitious attempts to influence their business decisions. Intelligence and national security agencies, which integrate counterintelligence and denial and deception into their analyses and operations, are perhaps more aware of the potential for foreign influence operations. However, the personnel who search for such influence activities generally do so by looking for falsehoods and misinformation in foreign statements and communications – not examining electronic data. Consequently, just as ISSOs receive technological training regarding computer forensics and metrics, they should receive sociological training to identify and evaluate the content of influence operations and techniques used for social engineering. ISSOs must improve their understanding of how adversaries may be attempting to influence decisions and policy debates.

It would be difficult, though not impossible, for skilled analysts to identify patterns in the content of messages that are sent to or across an organization's cyber infrastructure, particularly if they partner with security officers who can identify technical patterns such as message origins, targets, and language use. However, it is difficult to assess the content of the many messages that may cross an organization's servers on a daily basis, even if suspicious items are flagged by security officers. Artificial intelligence (AI) tools can be employed to scan incoming data for content and identifying information much more effectively and efficiently than humans can. Once patterns are identified, such tools can help systems keep up with adversaries' evolution by identifying changes to incoming messaging, delivery techniques, and other aspects of suspect communications. As influence messages are increasingly delivered and disseminated through electronic means – especially social media – both government and commercial organizations will need to employ electronic tools to defend against information attacks.

CONSEQUENCES OF PUTTING CYBER AND INFORMATION OPERATIONS IN SILOS

Cyber "bombs" started falling on Western population centers ten years ago, when Russia – in retaliation for the Estonian government's removal of a Soviet-era war memorial – launched a highly effective distributed denial of service (DDOS) attack on Estonia that brought down web sites of Estonian government agencies, banks, newspapers, and other organizations providing critical information and services. Since that first high-profile use of cyber tools to cause technical damage to networks, governments and companies have focused on defending themselves from similar attacks designed to impair their operations.

The consequences of this misalignment for the private sector – including the news media – is virtual blindness to direct information attacks conducted through a domain in which they are not fluent, leaving them unable to recognize an assault and leaving clients and media consumers unaware of (or even skeptical of) attack claims.

For its part, the public sector is effectively disarmed by its decision to align defensive cyber resources against the medium rather than the message. Government information security activities overwhelmingly focus on defending networks from technical attack but ignore strategic effects in the information space. Thus, although the citizenry might learn that foreign hackers or adversaries have tried to crack government networks X number of times, they remain generally unaware of hostile efforts to shape public perceptions through such technical attacks. (Recent reports of the extent of Russian manipulation of Facebook and Twitter during the 2016 campaign have only just begun to raise awareness of this threat.) This myopic focus on the technical means of attack rather than on the attacker's intended goal facilitates an adversary's ability to achieve its intended strategic effects through information operations.

CONCLUSIONS

Government agencies and private companies alike must take several steps to ensure they can recognize and defend themselves against hostile messages as well as hostile technical attacks. Organizations should:

1. Differentiate between attacks that target technical infrastructure and those that use technical infrastructure, and develop defense mechanisms customized to address each.

2. Train counterintelligence analysts and program managers in the analytic skills necessary to detect and counter influence operations.

3. Encourage more direct interaction between staff responsible for information security (such as ISSOs) and staff responsible for program security (such as counterintelligence officers). Greater collaboration between officials who separately focus on the technical medium of attack (cyber) and the impact of an attack (through messaging) would help organizations consider all motivations for attacks traversing cyber infrastructure, including theft, destruction, denial, deception, disruption, corruption, degradation, embarrassment, disinformation, and more.

4. Develop and deploy AI tools that are effective at scanning the content of incoming traffic for messages that could be attributed to hostile adversaries.

5. Promote collaboration between government researchers, academia, and private sector experts – perhaps in the form of a standing public-private partnership – to better educate the public of the threats posed by foreign influence operations. Identifying and characterizing foreign information and influence programs are often a government-sponsored activities that receive little public exposure. Similarly, academic and private sector research into these fields rarely receive wide recognition.

6. Foster closer engagement between the federal government and the media (including journalism schools) to teach journalists to identify information operations in their research. Particularly because of the hurried climate of the 24-hour news cycle, journalists can be directly exploited by adversaries or indirectly (and unintentionally) perpetuate fake news.

REFERENCES

[1]Keir Giles, Handbook of Russian Information Warfare, Rome: NATO Defense College, November 2016, p. 4. At https://krypt3ia.files.wordpress.com/2016/12/fm_9.pdf.

[2]Richard Kissel, ed., Glossary of Key Information Security Terms, NISTIR 7298, Rev. 2, Department of Commerce, National Institute of Standards and Technology, May 2013, p. 11. At http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

[3]President Franklin D. Roosevelt is widely cited as having asserted, "In politics, nothing happens by accident. If it happens, you can bet it was planned that way." The quotation may be apocryphal, but it applies equally to cyberspace as to politics.

[4]Giles, p. 4.

[5]Timothy L. Thomas, Recasting the Red Star: Russia Forges Tradition and Technology Through Toughness, Ft. Leavenworth, KS: Foreign Military Studies Office, 2011, pp. 141-150.

[6]National Intelligence Council, "Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent U.S. Elections," ICA 2017-01D, January 6, 2017, p. 2. At https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[7]Jen Weedon, William Nuland, and Alex Stamos, "Information Operations and Facebook," Facebook report, April 27, 2017. As of September 8, 2017: https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf.

[8]National Intelligence Council, p. 2.

[9]"Leaked Diplomatic Phone Conversation Generates Outrage Over U.S. Meddling in Ukraine," PBS NewsHour, February 7, 2014. At http://www.pbs.org/newshour/bb/leaked-diplomatic-phone-conversation-generates-outrage-american-meddling-ukraine/.

[10]Mike Isaac and Daisuke Wakabayashi, "Russian Influence Reached 126 Million Through Facebook Alone," New York Times, October 30, 2017. At https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html?_r=0.

[11]Carol D. Leonnig, Tom Hamburger, and Rosalind S. Helderman, "Russian Firm Tied to Pro-Kremlin Propaganda Advertised on Facebook During Election," Washington Post, September 6, 2017. At https://www.washingtonpost.com/politics/facebook-says-it-sold-political-ads-to-russian-company-during-2016-election/2017/09/06/32f01fd2-931e-11e7-89fa-bb822a46da5b_story.html?utm_term=.169274a4c860. See also Manu Raju, Dylan Byers, and Dana Bash, "Russian-Linked Facebook Ads Targeted Michigan and Wisconsin," CNN.com, October 4, 2017. At http://www.cnn.com/2017/10/03/politics/russian-facebook-ads-michigan-wisconsin/index.html. See also Alex Stamos, "An Update on Information Operations on Facebook," blog post, September 6, 2017. At https://newsroom.fb.com/news/2017/09/information-operations-update/.

[12]Scott Shane, "The Fake Americans Russia Created to Influence the Election," New York Times, September 7, 2017. At https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news.

[13]J.M. Berger, "Here's What Russia's Propaganda Network Wants You to Read," Politico, August 23, 2017. At https://www.politico.com/magazine/story/2017/08/23/russia-propaganda-network-kremlin-bots-215520.

[14]Ekaterina Blinova, "Unresolved Murder: Why Seth Rich's Case is Key to #TrumpRussia Investigation," Sputnik News, June 2, 2017. At https://sputniknews.com/politics/201706021054260081-seth-rich-trump-russia/.

ABOUT INSA

ABOUT THE INSA CYBER COUNCIL

INSA's Cyber Council seeks to lead, facilitate and deliver authoritative and influential insight around national security challenges present in the cyber domain by fusing knowledge from industry, government, and academic experts. The Council works to promote a greater understanding of cyber threats, challenges, and opportunities that can be addressed effectively through public-private collaboration.

ACKNOWLEDGEMENTS

This paper was developed and written by members of an Information Operations working group collaborating under the auspices of INSA's Cyber Council. Thanks are due to:

Richard Barger, *Splunk*

Cody Barrow

Mark Elliott, *Dependable Global Solutions*

Michael McMahon, *Leidos*

Admiral William O. Studeman, *USN (Ret.)*

Kevin Zerrusen, *Goldman Sachs; Cyber Council chair*

Appreciation is also due to INSA staff members who contributed to the publication:

Chuck Alsup, *President*

Larry Hanauer, *Vice President for Policy*

Ryan Pretzer, *Senior Manager, Policy and Public Relations*

Alexzandra Smith, *Intern*

INSA INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Building a Stronger Intelligence Community

(703) 224-4672 | www.INSAonline.org