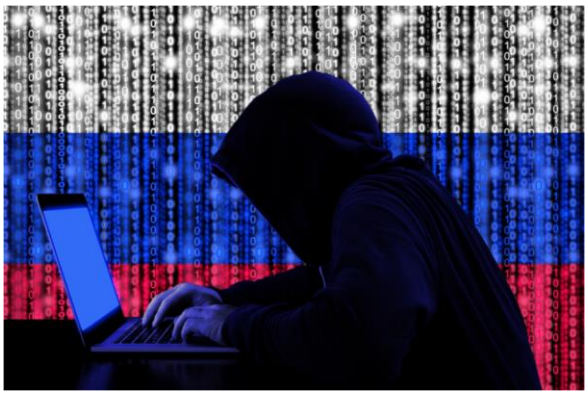
Old Tactics, New Tools:

A Review of Russia's Soft Cyber Influence Operations



Soviet propaganda mill spews out forgeries, fake news to undercut US

By John Dillin
Staff correspondent of
The Christian Science Monitor
September 22, 1983

A Minority Staff Report
Prepared for Democratic Members of the
Subcommittee on Oversight
Committee on Science, Space & Technology

November 2017

TABLE OF CONTENTS

Executive Summary	Page 1
Old (Soviet) Tactics, New (Russian) Tools	Page 5
Russian Reflexive Control Theory (RCT)	Page 6
Weaponizing Information	Page 7
• Sidebar: Weapons of Influence	Page 9
U.S. Intelligence Community Assessment (ICA)	Page 10
• Sidebar: Russian Virtual Reality	Page 11
Security Concerns about Kaspersky	Page 13
Hacking the U.S. Election Infrastructure	Page 15
Digital Trojan Horses	Page 19
Stoking Fears & Sowing Discontent	Page 20
Computer Code & Human Thought Code: Impact & Influence	Page 21
Countering Soft Cyber Influence Operations	Page 22

Executive Summary

The Committee on Science, Space & Technology recently held a hearing on the potential security threat posed by the use of Moscow-based Kaspersky Lab computer security products, particularly its well-known antivirus software.[1] The Committee will hold its second hearing on this topic on November 14, 2017.[2] There is bipartisan agreement that the use of Kaspersky Lab products poses a risk that federal agencies should not take. The Department of Homeland Security (DSH) issued a Binding Operational Directive (BDO) on September 13, 2017 that gave federal entities 90-days to initiate a plan to remove Kaspersky software from their computer networks.[3]

However, the Science Committee's recent focus on Kaspersky Lab, while important, loses sight of the much larger threat posed to the United States and other democracies from Russia's soft cyber influence operations. Russian information warfare strategy today is much broader than simply penetrating hard physical targets in order to acquire government, political or other data. Today, the Russians are using Soviet-era tactics and combining them with new digital tools, including trolls, bots and social media platforms to amplify their false and deceptive messages in order to influence democratic societies by discrediting democratic institutions and disrupting our democracy. Although the Russian influence campaign also targeted the U.S. election infrastructure during the 2016 US Presidential Campaign, those attempted cyber assaults were part and parcel of Russia's larger strategy to disrupt our democracy and deceive our citizenry. In September 2016, the Science Committee held a hearing on *"Protecting the 2016 Elections from Cyber and Voting Machine Attacks"* before the full extent of Russian interference became apparent.[4] As a result, the Ranking Member of the Science Committee, Ms. Eddie Bernice Johnson, and the Ranking Member of the Subcommittee on Oversight, Mr. Don Beyer, have both recently asked the Committee to conduct a post-mortem review of those attacks against our election infrastructure and the larger Russian influence campaign.[5]

Today, Russia is not simply targeting computers, but also human beings by weaponizing information in an effort to influence public opinion and encourage particular behavioral actions.

---

[1] *"Bolstering the Government's Cybersecurity: Assessing the Risk of Kaspersky Lab Products to the Federal Government,"* Subcommittee on Oversight, House Committee on Science, Space & Technology, October 25, 2017, accessed here: https://democrats-science.house.gov/legislation/hearings/bolstering-government-s-cybersecurity-assessing-risk-kaspersky-lab-products

[2] *"Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive,"* Subcommittee on Oversight, House Committee on Science, Space & Technology, November 14, 2017, accessed here: https://democrats-science.house.gov/legislation/hearings/bolstering-government-s-cybersecurity-survey-compliance-dhs-directive

[3] "DHS Statement on the Issuance of Binding Operational Directive 17-01," Office of the Press Secretary, Department of Homeland Security (DHS), September 13, 2017, accessed here: https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01

[4] *"Protecting the 2016 Elections from Cyber and Voting Machine Attacks,"* Subcommittee on Oversight, House Committee on Science, Space & Technology, September 13, 2017, accessed here: https://democrats-science.house.gov/legislation/hearings/protecting-2016-elections-cyber-and-voting-machine-attacks

[5] See the Opening Statements of Ms. Johnson and Mr. Beyer at the Subcommittee on Oversight hearing titled, *"Bolstering the Government's Cybersecurity: Assessing the Risk of Kaspersky Lab Products to the Federal Government,"* October 25, 2017, accessed here: https://democrats-science.house.gov/legislation/hearings/bolstering-government-s-cybersecurity-assessing-risk-kaspersky-lab-products

These influence campaigns combine using cyber technologies to infiltrate computer networks in order to acquire or corrupt data along with efforts that seek to heighten social discord, amplify Russian produced disinformation, and create distrust of democratic institutions, particularly a free and fair media, via multiple communications technologies and social media platforms.

The Russian influence campaign that occurred during the 2016 US Presidential election is a key example of this emerging practice of what this report refers to as soft cyber influence operations. Russia has used these same tactics in recent years against other democracies, particularly in Europe, including in France, Germany, Ukraine and Estonia, for instance. In the United States they attempted to penetrate voter databases prior to the 2016 Election, successfully penetrated the Democratic National Committee (DNC) network, and accessed state-level Republican organizations and candidates.

Once the DNC was successfully penetrated and its cache of e-mails released via Wikileaks the Russian influence campaign flooded social media sites with disinformation and false news stories. They choreographed an elaborate influence campaign that soughtto undercut the Democratic Presidential candidate Hillary Clinton and undermine our democracy.[6] In 2014 Russian-linked actors also compromised the Central Election Committee's computer network in Ukraine.[7] Russia used these cyber-assaults and their coordinated influence campaigns to help convey a message of division, distrust and doubt regarding the validity and legitimacy of core democratic institutions. They sought to damage and sow distrust in the democratic electoral process, the most basic and fundamental pillar of our Constitution and democracy.

This report examines Soviet-era propaganda tactics and information warfare strategy that are being used by Russia today. It details how Russian military strategists have foreshadowed the use of information as a weapon for decades, highlighting how information could be used to undermine democratic institutions. The methods these analysts laid out appear to coincide with actual actions the Russian intelligence services engaged in during the 2016 US Presidential Election and in other soft cyber attacks they have waged against other democratic nations. This report also examines new efforts to identify and confront these evolving and expanding threats.

Three decades ago, in the early 1980s, the House Permanent Select Committee on Intelligence (HPSCI) held several hearings on the Soviet Union's "active measures" and "covert actions" against the United States and our Western allies. Strikingly, the tactics they employed then, including forgeries, disinformation campaigns and fake news, are eerily similar to the recent revelations over the past eighteen months about Russia's efforts to influence and disrupt the 2016 U.S. Presidential Election.[8] The headline of a newspaper story published in the *Christian Science*

---

[6] Evan Osnos, David Remnick, and Joshua Yaffa, "Trump, Putin, and The New Cold War: What lay behind Russia's interference in the 2016 election—and what lies ahead?" *The New Yorker*, March 6, 2017, accessed here: https://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war

[7] Pascal Brangetto and Matthijs A. Veenendaal, "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations," NATO Cooperative Cyber Defense Centre of Excellence, Tallinn, Estonia, presented at the 2016 8th International conference on Cyber Conflict, accessed here: https://ccdcoe.org/cycon/2016/proceedings/08_brangetto_veenendaal.pdf

[8] See: *"Soviet Active Measures,"* Hearings before the Permanent Select Committee on Intelligence, U.S. House of Representatives, Ninety-Seventh Congress, Second Session, July 14 and July 18, 1982 and *"Soviet Covert Action*

Monitor in September 1983 was titled: *"Soviet propaganda mill spews out forgeries, fake news to undercut US."*[9] That headline could have replaced "Soviet" with "Russia" and been printed in 2017.

Recent Russian efforts to undercut our democracy should not have come as a surprise. According to a Czechoslovak intelligence officer who defected to the United States in 1968, and testified before the HPSCI in 1980, during the 1964 U.S. Presidential Election the Czech intelligence service, acting under the direction of the Soviet Union's KGB, produced fake leaflets distributed in the U.S. to target Republican Presidential candidate Barry Goldwater.[10] More than 50 years later Russia's FSB intelligence service used similar Soviet-era strategies and tactics and combined them with new digital-era tools to target Democratic Presidential candidate Hillary Clinton.

Since at least the late 1990s and early 2000s Russian strategic military analysts have been writing in Russian language journals about the use of information warfare-related tactics to influence democratic elections. Russia has a much broader concept of "information warfare" than the United States. The recent Russian efforts to influence the electoral process in the United States, France, Germany, Ukraine, Latvia and other nations is based on the concept of "Reflexive Control Theory (RCT)." The concept was first developed by Vladimir Lefebvre, described as a "mathematical psychologist," to apply the science of social psychology to national security related issues.[11] According to Timothy L. Thomas, one of the foremost experts on RCT in the United States, "Reflexive control is defined as a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action."[12] The Russians sought to use reflexive control strategies to influence the behavior of American voters at the ballot box.

The concept of RCT as a strategic blueprint for undermining democracies through the use of information warfare techniques can be seen both in the writings of Russian military strategists and in the actions of the Russian intelligence service and their surrogates during the 2016 U.S. Presidential Election. In 2001, one Russian strategic analyst wrote that emerging information technologies would make it possible to distort a group or even a country's reality by imposing alternative "facts" into the society. These actions could help undermine citizens' trust in their government or specific actions taken by the government as well as in the "mass media, which are called upon to be a source of objective information," the author wrote. "The direct result of this feature of the use of information weapons is that the country's supreme leadership as well as

---

(The Forgery Offensive)," Hearings before the Permanent Select Committee on Intelligence, U.S. House of Representatives, Ninety-Sixth Congress, Second Session, February 6, 19, 1980.

[9] John Dillan, "Soviet propaganda mill spews out forgeries, fake news to undercut US," *Christian Science Monitor*, September 22, 1983.

[10] *"Soviet Covert Action (The Forgery Offensive),"* Hearings before the Permanent Select Committee on Intelligence, U.S. House of Representatives, Ninety-Sixth Congress, Second Session, February 6, 19, 1980.

[11] See: Brief Biography of Vladimir A. Lefebvre, accessed here: http://www.armsada.eu/pb/vlfIASCYSpageEN.pdf; and here: https://mipt.ru/education/chairs/theor_cybernetics/government/upload/ebd/InsidetheTank-arpgk4cl061.pdf; and http://www.1260.org/Mary/People/People_Lefebvre_Vladimir_en.htm

[12] Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies*, 2004, accessed here: https://www.rit.edu/~w-cmmc/literature/Thomas_2004.pdf

society as a whole may not know just what really is happening."[13] In 2004, another Russian author wrote that employing information weapons "will make it possible to influence the outcome of presidential elections, to form public opinion, and to exert pressure on processes capable of ensuring bloodless and effective control of states from the outside."[14]

Despite recent denials by President Trump that Russia did not interfere in the 2016 Presidential Elections there is ample evidence to the contrary on record.[15] Russian intelligence has used a wide-range of tactics to influence and disrupt not just the democratic electoral process in the United States but democratic societies as a whole. They have concocted fake news and even fake people to help them disseminate disinformation through a wide range of social media platforms.[16] They have done this in combination with cyber-attacks against various targets including political institutions and election-related systems. The efforts appear wider than simply influencing one election. They appear to have also sought to sow divisions among the public, and to discredit democratic institutions and trust in the integrity of our democratic institutions.

Just last month, former President George W. Bush said: "[T]he Russian government has made a project of turning Americans against each other. This effort is broad, systematic and stealthy, it's conducted across a range of social media platforms. …. We must secure our electoral infrastructure and protect our electoral system from subversion," he warned.[17]

Science and technology can help play a pivotal role in identifying and defending against these attacks in the future. The Russians have utilized a keen understanding of social science in an attempt to influence the public in democratic societies and inflame divisions among its citizens. Faced with this new reality the United States must understand this threat, be able to identify it and defend against it. This will entail combined efforts by behavioral social scientists, cybersecurity experts and technologists. These are issues the Science Committee should examine closely and carefully to offer support and congressional oversight where appropriate.

---

[13] "Information Weapons as a New Means of Warfare" (Chapter 3) from book "Information Challenges to National and International Security," edited by Candidate of Physicomathematical Sciences Aleksandr V. Fedorov and Doctor of Technical Sciences, Professor, Russian Academy of Natural Sciences, Academician Vitaliy N. Tsygichko, Moscow PIR Center, August 1, 2001, pp. 69-109 (in Russian). The Russian Center for Policy Research (PIR Center) is a Moscow-based nonprofit organization.

[14] Boris Rodionov, "Future 'Weapons of Influence' to Control Elections," Armeyskiy Sbornik, Moscow, (in Russian), October 31, 2004 (monthly journal of the General Staff of the Russian Federation Armed Forces).

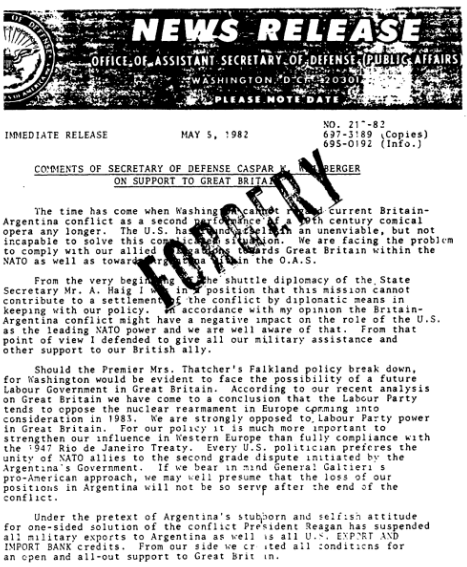
[15] See: Kevin Liptak and Dan Merica, "Trump says he believes Putin's election meddling denials," CNN, November 12, 2017, accessed here: http://www.cnn.com/2017/11/11/politics/president-donald-trump-vladimir-putin-election-meddling/index.html; and "Assessing Russian Activities and Intentions in Recent US Elections," U.S. Intelligence Community Assessment (ICA), Office of the Director of National Intelligence (ODNI), National Intelligence Council, January 6, 2017, accessed here: https://www.dni.gov/files/documents/ICA_2017_01.pdf

[16] Scott Shane, "The Fake Americans Russia Created to Influence the Election," *New York Times*, September 7. 2017, accessed here: https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html

[17] Transcript of speech delivered by former President George W. Bush at the *"Spirit of Liberty"* forum held at Lincoln Center in New York City, October 19, 2017, accessed here: https://www.usnews.com/news/articles/2017-10-19/transcript-george-w-bush-calls-out-donald-trumps-america-russian-aggression

Old (Soviet) Tactics, New (Russian) Tools

The tactics that have recently been employed by Russia in Georgia, Ukraine, Estonia, Germany, France and during the 2016 Presidential election in the United States are nothing new. The Russians have taken old Soviet-era tactics and refreshed them, refined them and improved them by using new information technologies, such as social media, and exploiting the global digital connections of the Internet. In July 1982, during a series of public hearings before the House Permanent Select Committee on Intelligence (HPSCI), titled *"Soviet Active Measures,"* the Central Intelligence Agency (CIA) revealed a litany of Soviet forgeries, including a U.S. Department of Defense press release, documents from the U.S. Department of Commerce and State Department, and a letter from President Reagan to the King of Spain. These efforts also included disinformation, or fake information, to help deceive and confuse the United States, that included maps of Afghanistan and Cuba.[18]



NEWS RELEASE

OFFICE OF ASSISTANT SECRETARY OF DEFENSE (PUBLIC AFFAIRS)

WASHINGTON, D.C. 20301

PLEASE NOTE DATE

IMMEDIATE RELEASE MAY 5, 1982

NO. 217-82
697-3189 (Copies)
695-0192 (Info.)

COMMENTS OF SECRETARY OF DEFENSE CASPAR W. WEINBERGER
ON SUPPORT TO GREAT BRITAIN

The time has come when Washington cannot afford current Britain-Argentina conflict as a second performance of a 19th century comical opera any longer. The U.S. has found itself in an unenviable, but not incapable to solve this conflicting situation. We are facing the problem to comply with our allied obligations towards Great Britain within the NATO as well as toward Argentina within the O.A.S.

From the very beginning of the shuttle diplomacy of the State Secretary Mr. A. Haig I was in a position that this mission cannot contribute to a settlement of the conflict by diplomatic means in keeping with our policy. In accordance with my opinion the Britain-Argentina conflict might have a negative impact on the role of the U.S. as the leading NATO power and we are well aware of that. From that point of view I defended to give all our military assistance and other support to our British ally.

Should the Premier Mrs. Thatcher's Falkland policy break down, for Washington would be evident to face the possibility of a future Labour Government in Great Britain. According to our recent analysis on Great Britain we have come to a conclusion that the Labour Party tends to oppose the nuclear rearmament in Europe coming into consideration in 1983. We are strongly opposed to Labour Party power in Great Britain. For our policy it is much more important to strengthen our influence in Western Europe than fully compliance with the 1947 Rio de Janeiro Treaty. Every U.S. politician prefers the unity of NATO allies to the second grade dispute initiated by the Argentina's Government. If we bear in mind General Galtieri's pro-American approach, we may well presume that the loss of our positions in Argentina will not be so serve after the end of the conflict.

Under the pretext of Argentina's stubborn and selfish attitude for one-sided solution of the conflict President Reagan has suspended all military exports to Argentina as well as all U.S. EXPORT AND IMPORT BANK credits. From our side we created all conditions for an open and all-out support to Great Britain.

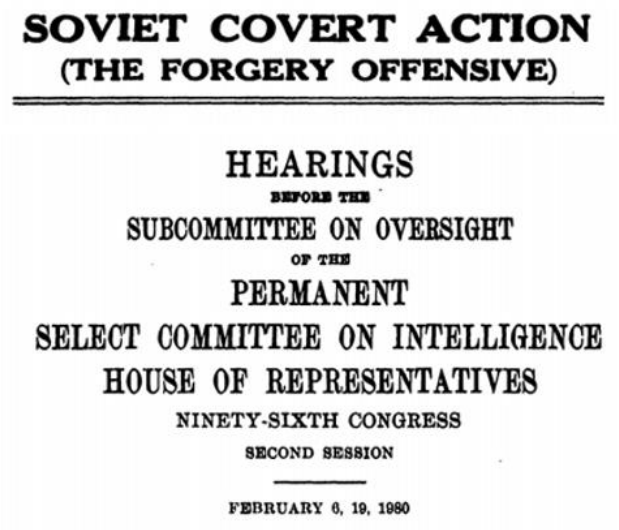
FORGERY

Even more relevant and revealing regarding Russian cyber influence activities during the 2016 Presidential Elections, in February 1980 HPSCI held another set of hearings titled, *"Soviet Covert Action (The Forgery Offensive)."* One of the key witnesses was Ladislav Bittman, former Deputy Chief of the Disinformation Department of the Czechoslavia Intelligence Service. In 1968 Bittman defected to the United States. The Czech intelligence services and those of the Soviet Union, known as the KGB, worked closely together. Mr. Bittman was asked about a propaganda operation in 1964 against Senator Barry Goldwater, who was then a Republican candidate for President of the United States. The operation was carried out by the Czech intelligence service at the direction of the KGB. Bittman said:

> Well, the operation conducted by the Czechoslovak intelligence was, considering the election process in this country, the tremendous amount of information flooding the American public, this operation was a drop into an ocean of anti-Goldwater feeling, genuine feelings in the United States. It was a booklet or leaflet produced by the Czech service.
>
> In the text there were some genuine statements by Goldwater and then some statements which were manufactured indicating his racism. Mainly it was supposed racist policies or whatever, and this was then distributed in the United States and also abroad.[19]

[18] "Soviet Active Measures," Hearings before the Permanent Select Committee on Intelligence, U.S. House of Representatives, Ninety-Seventh Congress, Second Session, July 14 and July 18, 1982.
[19] "Soviet Covert Action (The Forgery Offensive)," Hearings before the Permanent Select Committee on Intelligence, U.S. House of Representatives, Ninety-Sixth Congress, Second Session, February 6, 19, 1980.

The hearing also divulged that the KGB had produced a fake CIA document reportedly showing the CIA had more than five dozen American journalists from the *New York Times*, *Washington Post* and many other publications on its payroll.[20] The tactics and goals of the former Soviet Union during the Cold War have been replaced by new tools and technologies that have helped Russia carry out similar disinformation and cyber influence operations today.


SOVIET COVERT ACTION
(THE FORGERY OFFENSIVE)

HEARINGS
BEFORE THE
SUBCOMMITTEE ON OVERSIGHT
OF THE
PERMANENT
SELECT COMMITTEE ON INTELLIGENCE
HOUSE OF REPRESENTATIVES
NINETY-SIXTH CONGRESS
SECOND SESSION

FEBRUARY 6, 19, 1980

Reflexive Control Theory (RCT)

The Russian approach to information warfare related issues is much broader, and in many ways, much more sophisticated, than the Western concepts of cybersecurity and information warfare. The Russian theory of Reflexive Control (RC) is at the heart of Russia's information warfare tactics. The theory has often been defined as, "a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision." The concept was first developed by Vladimir A. Lefebvre, described as a mathematical psychologist whose books include the "Algebra of Conscience" and "Reflexive Control: The Soviet Concept of Influencing an Adversary's Decision Making Process."[21] Lefebvre developed the concept in the mid-1960s when he was at the Military Institute of Electronics in Moscow.[22] Lefebvre came to the United States in the 1970s and is a researcher in cognitive science at the School of Social Sciences at the University of California in Irvine.[23] Lefebvre has noted, "The main condition for success in this propagandistic influence is masking the very fact of influence."[24] Thus, there is a covert or clandestine element to RC theory.

The American military began studying Russian reflexive control strategies and tactics in the 1980s. In July 1986 Diane Chotikul, a researcher in the Department of Operations Research at the Naval Postgraduate School in Monterey, California published a report titled, "The Soviet Theory of Reflexive Control in Historical and Psychocultural Perspective: A Preliminary Study."[25] In 1985, the Department of Defense used the term "Reflexive Control" in a report they submitted to Congress on Soviet Strategic Deception. That study evaluated areas where the

[20] See: "Paid CIA Agents, Sources of Information or Assistance in the World Mass Media," pages 173-195 in "Soviet Active Measures," Hearings before the Permanent Select Committee on Intelligence, U.S. House of Representatives, Ninety-Seventh Congress, Second Session, July 14 and July 18, 1982. (The fake CIA, KGB produced, document listed hundreds of journalists in dozens of countries around the world.)
[21] Diane Chotikul, *"The Soviet Theory of Reflexive Control in Historical and Psychocultural Perspective: A Preliminary Study,"* Naval Postgraduate School, Monterey, California, July 1986, accessed here: http://www.dtic.mil/dtic/tr/fulltext/u2/a170613.pdf
[22] See bio of Vladimir A. Lefebvre posted at the Associations for the Reciprocal and Mutual Sharing of Advantages and DisAdvantage (ARMSADA), accessed here: shttp://www.armsada.eu/pb/vlfIASCYSpageEN.pdf
[23] See, Vladimir Lefebvre. University of California at Irvine, accessed here: https://www.faculty.uci.edu/scripts/UCIFacultyProfiles/detailMBB.cfm?ID=5130
[24] Op. Cit.
[25] Op. Cit.

United States was "most vulnerable to Soviet deception and manipulation as an active program of 'reflexive control,'" the report said.[26]

Timothy L. Thomas who recently retired as a senior analyst at the Army's Foreign Military Studies Office at Ft. Leavenworth is one of the foremost experts on Russian Reflexive Control. He testified before Congress on March 15, 2017, about Russia's information warfare activities.

> "Russia's information warfare approach is holistic. It is focused not only on media and propaganda, but on information technologies that fit weaponry as well. Ever since the 1990s, Russia has divided its information warfare concepts into two parts: Information technical and information psychological. Social media and cyber have tended to blend the two and caused a significant change in how Russia views the emerging trends in the character of warfare. …. Methods are composed of two parts: Weaponry and military art. Weaponry can include hackers, reflexive control techniques, trolls, disinformation, deterrence capabilities, and other agents of destruction or influence. Military art includes the use of indirect and asymmetric capabilities to achieve specific goals, such as the exploitation of the West's free press or an indirect attack on the cyber infrastructure of another nation. Russian's excellent contingent of algorithm writers ensures that the nation will be strong for years to come in writing software as weapons that could eavesdrop, persuade, or destroy.[27]

Weaponizing Information

The Internet has provided the digital tentacles that can reach virtually anyone, anywhere in the world with the touch of a button. At the same time, social media platforms have augmented the ability to provide a kaleidoscope of disinformation, distortions and fake news that can be amplified and directed towards specific audiences. This has become a powerful weapon that can target individuals or specific groups everywhere. "Across the world, the weaponization of information is becoming a major trend and a significant threat," said a 2015 report from the Center for European Policy Analysis (CEPA). The report described some of the Russian tactics in this new information war as follows: "Dismiss the critic; Distort the facts; Distract from the main issue; and Dismay the audience."[28] Many other publications and reports, as well as

---

26 "Soviet Active Measures," Hearings before the Permanent Select Committee on Intelligence, U.S. House of Representatives, Ninety-Seventh Congress, Second Session, July 14 and July 18, 1982.

[27] Timothy L. Thomas, Written Testimony for the hearing titled: "Crafting an Information Warfare and Counter-Propaganda Strategy for the Emerging Security Environment," Subcommittee on Emerging Threats and Capabilities, House Armed Services Committee, March 15, 2017, accessed here: http://docs.house.gov/meetings/AS/AS26/20170315/105689/HHRG-115-AS26-Wstate-ThomasT-20170315.pdf

[28] "How Has Russia Weaponized Information," Center for European Policy Analysis, November 2015, accessed here: http://cepa.org/index/?id=6060d322713797e84f598ea25c812cab and here: http://cepa.org/sites/default/files/Infowar%20Report.pdf.

academics, have also described the weaponization of information by Russia.[29] In April 2015, the House Foreign Affairs Committee even held a hearing titled: "Confronting Russia's Weaponization of Information."[30] The CEPA report noted, "Russian disinformation does not aim to provide answers, but to provoke doubt, disagreement and, ultimately, paralysis." It is "calibrated to confuse, befuddle and distract," the report concluded.[31]

As the sidebars on the following pages show, Russian military strategists have been contemplating how to use information as a weapon against Western democracies for many years. In fact, some of these analysts appear to have telegraphed the types of information attacks that occurred during the 2016 U.S. Presidential elections. Ironically, American technical innovation, particularly the creation of the Internet and the more recent development of social media platforms, such as Facebook, Twitter, Instagram and others, has created the tools that have allowed Russian intelligence officers to put the designs of Russian strategic thinkers into practice.

Many Russian observers have also written about the broad Russian approach to Information Warfare. "While the West understands cyberspace capabilities as mostly technical," Piret Pernik, the former advisor to the National Defense Committee of the Estonia Parliament and a Research

[29] See: Peter Pomerantsev and Michael Weiss, "The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money," *The Interpreter*, a project of the Institute of Modern Russia, November 2014, accessed here: http://www.interpretermag.com/wp-content/uploads/2014/11/The_Menace_of_Unreality_Final.pdf; "Weaponizing Information Conference," sponsored by the Center for Global Legal Challenges and the Information Society Project both affiliated with the Yale Law School, January 24, 2017, accessed here: https://law.yale.edu/yls-today/news/weaponizing-information-conference-watch-panel-videos; "Weaponization of information key part of Russian military doctrine," Neil MacFarquhar, *New York Times*, August 28, 2016, accessed here: https://www.seattletimes.com/nation-world/weaponization-of-information-key-part-of-russian-military-doctrine/; Fred Kaplan, "The Info Wars to Come: Russia is weaponizing social media. It's time we started defending ourselves." *Slate*, September 8, 2017, accessed here: http://www.slate.com/articles/news_and_politics/war_stories/2017/09/russia_is_weaponizing_social_media.html

[30] *"Confronting Russia's Weaponization of Information,"* House Foreign Affairs Committee, April 15, 2015, accessed here: https://foreignaffairs.house.gov/hearing/hearing-confronting-russias-weaponization-of-information/

[31] "How Has Russia Weaponized Information," Center for European Policy Analysis, November 2015, accessed here: http://cepa.org/index/?id=6060d322713797e84f598ea25c812cab; and here: http://cepa.org/sites/default/files/Infowar%20Report.pdf;

Fellow at the International Centre for Defense and Security in Tallinn, Estonia, told *The Cipher Brief*, "the Russian understanding of the information domain includes electronic warfare and intelligence capabilities, as well as measures such as disinformation, propaganda, psychological pressure, destabilization of society, and influence of foreign media."[32]

Margarita Jaitner, an information warfare researcher at the Swedish Defense University, has written about Russian's use of information attacks in Ukraine. "In Ukraine, 'conventional' cyber attacks by Russia were negligible, but social media-based, narrative-focused attacks including disinformation have been common."[33] Dr. Constanze Stelzenmüller, a Senior Fellow at Brookings Institution testified before the Senate Select Committee on Intelligence regarding the impact of Russian interference in Germany's 2017 elections. She noted, "A hacking of voting technology in the German elections probably can't be excluded completely; but experts concur it is highly unlikely to succeed. Voters' heads are by far the more vulnerable target," she said.[34]

Weapons of Influence

Boris Rodionov, **"Future 'Weapons of Influence' to Control Elections,"** *Armeyskiy Sbornik*, Moscow, (in Russian), October 31, 2004 (monthly journal of the General Staff of the Russian Federation Armed Forces).

"Basic focus undoubtedly will be put on forced introduction of foreign information into the human brain. **This will make it possible to influence the outcome of presidential elections, to form public opinion, and to exert pressure on processes capable of ensuring bloodless and effective control of states from the outside.**

[Rodionov describes the rise of "weapons of influence" in the 21st century.]

Using such weapons**, it will be possible to exert long-range controlling effects on persons, and consequently on the course and results of election campaigns, on the decision-making of presidents,** prime minister, and other high-ranking persons, and in this way to control the entire world."

[32] Levi, Maxey, "The Baltics: Veterans of Russian Cyber Operations," *The Cipher Brief*, March 19, 2017, accessed here: https://www.thecipherbrief.com/the-baltics-veterans-of-russian-cyber-operations

[33] Margarita Jaitner, "Russian Information Warfare: Lessons from Ukraine," NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), November 2015, accessed here: https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Jaitner_10.pdf

[34] Constanze Stelzenmüller, "The impact of Russian interference on Germany's 2017 elections," testimony before the U.S. Senate Select Committee on Intelligence, June 28, 2017, accessed here: https://www.intelligence.senate.gov/sites/default/files/documents/sfr-cstelzenmuller-062817b.pdf;

U.S. Intelligence Community Assessment (ICA)

The U.S. Intelligence Community Assessment (ICA) published in January 2017, titled: *"Assessing Russian Activities and Intentions in Recent US Elections,"* stated: "We also assess Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him."[35] This assessment fits neatly with what Russian strategic thinkers have said about how they could utilize information as a weapon to undermine or boost public support for particular candidates in democratic societies in the past. In 2001, Aleksandr V. Fedrov and Vitaliy N. Tsygichko, wrote: "By supplying positive information through the mass media about one's contender for some position and simultaneously creating a good psychophysical state of the population …. it is possible to develop a positive conditioned reflex to this contender in the population and substantially increase his popularity because of this." The authors continued, "It's [also] possible to develop a negative conditioned reflex to this nominee by providing negative information about an undesirable nominee and at the same time creating a negative psychophysical state in people…."[36]

Earlier this month the *Associated Press* analyzed Twitter accounts linked to Russia that found these sorts of tactics in play during the 2016 US Presidential Election, particularly after the public release of the 2005 "Access Hollywood" audiotape which revealed crude sexual comments by Donald Trump. As the media began to report on release of this tape, Russian trolls went into action. Russia sought to redirect negative attention on Donald Trump towards Hillary Clinton. "Disguised Russian agents on Twitter rushed to deflect scandalous news about Donald Trump just before last year's presidential election," the *AP* reported, "while straining to refocus criticism on the mainstream media and Hillary Clinton's campaign." The *AP* examined 36,210 tweets from August 31, 2015, to November 10, 2016, posted by 382 Russian accounts that Twitter has since deactivated. The *AP* was only able to access a portion of the tweets from these accounts. Some of these Twitter accounts had tens of thousands of followers which helped to amplify the false messages they were sending and expanded the impact and influence of each

[35] "Assessing Russian Activities and Intentions in Recent US Elections," U.S. Intelligence Community Assessment (ICA), Office of the Director of National Intelligence (ODNI), National Intelligence Council, January 6, 2017, accessed here: https://www.dni.gov/files/documents/ICA_2017_01.pdf

[36] "Information Weapons as a New Means of Warfare" (Chapter 3) from book "Information Challenges to National and International Security," edited by Candidate of Physicomathematical Sciences Aleksandr V. Fedorov and Doctor of Technical Sciences, Professor, Russian Academy of Natural Sciences, Academician Vitaliy N. Tsygichko, Moscow PIR Center, August 1, 2001, pp. 69-109 (in Russian). The Russian Center for Policy Research (PIR Center) is a Moscow-based nonprofit organization.

false or distorted tweet. They successfully turned a band of a few hundred Russian agents into an army of tens of thousands of followers.[37]

"Moscow's influence campaign followed a Russian messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or "trolls," concluded the ICA of Russia's influence campaign. "Russia, like its Soviet predecessor, has a history of conducting covert influence campaigns focused on US presidential elections that have used intelligence officers and agents and press placements to disparage candidates perceived as hostile to the Kremlin," the report said. [Emphasis in the original].[38]

As Timothy Thomas observes in a paper he wrote titled, "Russia's 21st Century Information War: Working to Undermine and Destabilize Populations," Russia uses tactics of deception, propaganda and other modes of influence in an attempt to create an "alternative reality." Russian government influence operatives and strategists seek to manipulate the flow of information into specific social environments in order to concoct a virtual reality. "Russia uses its techniques to alter the landscape of objectivity

Russian Virtual Reality

"Information Weapons as a New Means of Warfare" (Chapter 3) from book "Information Challenges to National and International Security," edited by Candidate of Physicomathematical Sciences Aleksandr V. Fedorov and Doctor of Technical Sciences, Professor, Russian Academy of Natural Sciences, Academician Vitaliy N. Tsygichko

Moscow PIR Center, August 1, 2001, pp. 69-109 (in Russian). The Russian Center for Policy Research (PIR Center) is a Moscow-based nonprofit organization.

"There is the possibility that the "facts" of a particular event will be seriously distorted by textual, audio and video information techniques. Such methods can allow a wide range of interested persons or groups to accomplish a complicated process of regulating public perception or organizing major propaganda campaigns to undermine citizens' trust in a specific course being taken by the country's government. A campaign of this nature poses serious problems not only for the government, but also for the mass media, which are called upon to be a source of objective information. The direct result of this feature of the use of information weapons is that the country's supreme leadership as well as society as a whole may not know just what really is happening."

[37] Ryan Nakashima and Barbara Ortutay, "AP Exclusive: Russia Twitter trolls deflected Trump bad news," *The Washington Post*, November 8, 2017, accessed here: https://www.washingtonpost.com/business/technology/ap-exclusive-russia-twitter-trolls-deflected-bad-trump-news/2017/11/09/cab7945c-c560-11e7-9922-4151f5ca6168_story.html?utm_term=.293590095d84

[38] "U.S. Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections," Office of the Director of National Intelligence, ICA 2017-01D, January 6, 2017, accessed here: https://www.dni.gov/files/documents/ICA_2017_01.pdf

and transform it into a new reality of its own making…." observes Thomas.[39] "To them," Thomas observed in prepared remarks to the House Armed Services Committee in March 2017, referring to the Russian government, "reality is negotiable."[40] Journalists Peter Pomerantsev and Michael Weiss have also written about this observation. "The underlying mindset of the Kremlin's political technologists exploits the idea that "truth" is a lost cause and that reality is essentially malleable, and the instant, easy proliferation of fakes and copies on the Internet makes it the ideal forum to spread such ideas," they wrote.[41]

Russia has tried to shape the reality they want by combining their cyber assaults with influence operations, and to a large degree they have been successful. "Russia, more than any other nascent actor on the cyber stage, seems to have devised a way to integrate cyber warfare into a grand strategy capable of achieving political objectives," wrote James J. Wirtz, Dean of the Naval Postgraduate School in California, in a publication for NATO in 2015.[42] Others have also described how Russia has effectively integrated its cyberattack operations with its foreign influence campaigns. Pascal Brangetto and Matthijs A. Veenendaal both from NATO's Cooperative Cyber Defense Centre of Excellence (CCD COE) in Tallinn, Estonia, offered a study at the 2016 8th International Conference on Cyber Conflict titled: "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations."[43] They coined the term Influence Cyber Operations (ICO) to describe these actions. In this report the term Soft Cyber Influence Operations is used to describe similar tactics. Dr. Tim Stevens of Kings College London sums up this strategy underlying these sorts of influence operations this way, "Cyberwarfare of the future may be less about hacking electrical power grids and more about hacking minds by shaping the environment in which political debate takes place."[44]

---

[39] Timothy Thomas, "Russia's 21st Century Information War: Working to Undermine and Destabilize Populations," Defence Strategic Communications (The official journal of the NATO Strategic Communications Centre of Excellence), Volume 1, Number 1, Winter 2015, accessed here: https://www.stratcomcoe.org/timothy-thomas-russias-21st-century-information-war-working-undermine-and-destabilize-populations

[40] Prepared Statement. Timothy Thomas, Senior Analyst, Foreign Military Studies Office, Fort Leavenworth, Before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, March 15, 2017, accessed here: http://docs.house.gov/meetings/AS/AS26/20170315/105689/HHRG-115-AS26-Wstate-ThomasT-20170315.pdf

[41] Peter Pomerantsev and Michael Weiss, "The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money," Interpreter, November 22, 2014, http://www.interpretermag.com/wp-content/uploads/2014/11/The_Menace_of_Unreality_Final.pdf

[42] James J. Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy," Chapter 3 in Kenneth Geers (Ed.), Cyber War in Perspective: Russian Aggression against Ukraine, NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), Tallinn, Estonia, 2015, accessed here: https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Wirtz_03.pdf

[43] Pascal Brangetto and Matthijs A. Veenendaal, "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations," NATO Cooperative Cyber Defense Centre of Excellence, Tallinn, Estonia, presented at the 2016 8th International conference on Cyber Conflict, accessed here: https://ccdcoe.org/cycon/2016/proceedings/08_brangetto_veenendaal.pdf

[44] Ibid.

Security Concerns about Kaspersky

Combined with aggressive Russian cyber-attacks against hard targets, such as power plants, Russia's sophisticated soft cyber influence operations have led to mounting concerns about Russian cyber targets and the tactics being employed against the U.S. and other democracies. This may have heightened U.S. concerns about the use of Kaspersky Lab products, particularly antivirus software by federal agencies recently. Kaspersky Lab is a Russian owned and operated cybersecurity firm based in Moscow, and its software is used by an estimated 400 million users and 270,000 corporate clients around the world. The founder and owner of Kaspersky Lab, Eugene Kaspersky, is a software engineer who was educated at a KGB cryptography institute and later worked for the Russian intelligence service prior to starting Kaspersky Lab in 1997. Kaspersky has been described as the "Bill Gates of Russia" and since 2015 has been on Forbes' Billionaires List.[45]

In July 2017, the General Services Administration (GSA) removed Kaspersky Lab from a list of approved federal government vendors. This move prevented federal agencies from using GSA contracts to procure Kaspersky Lab products and services. On September 13, 2017, DHS issued a Binding Operational Directive (BOD) banning the use of Kaspersky products by U.S. government entities. All federal agencies are required to remove Kaspersky products from their networks by mid-December. The directive said DHS was concerned about ties between Kaspersky and Russian intelligence, combined with the fact that Kaspersky products constitute information security risks because by their very nature they open the door to access a network's data. However, the specific technical concerns and details on "ties" with Russian intelligence cited in the BOD were very vague. "The risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to compromise federal information and information systems directly implicates U.S.

[45] See: Noah Shachtman, "Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals," *WIRED*, July 23, 2012, accessed here: https://www.wired.com/2012/07/ff_kaspersky/

national security," said the official DHS press release on the Binding Operational Directive.[46] Detailed information regarding the U.S. intelligence community's security concerns about Kaspersky are classified. Kaspersky Lab has said it has no ties to *any* government.

U.S. security concerns about Kaspersky Lab appear to have heated up in recent months. In April, the Senate Intelligence Committee reportedly asked the Director of National Intelligence and U.S. Attorney General to look into Kaspersky employees' relationship with Russian intelligence agencies.[47] On May 11th, six U.S. intelligence agency directors, including the Director of National Intelligence, CIA, NSA and Acting Director of the FBI, all told the Senate Intelligence Committee that they would not be comfortable using Kaspersky products on their networks.[48] In June multiple media reports said FBI agents had interviewed at least one dozen U.S. based employees of Kaspersky Lab.[49] In October, the *New York Times* also reported that Israeli intelligence had themselves penetrated Kaspersky Lab's antivirus software and were able to determine that Russian government hackers were using the company's software to search for the code names of American intelligence programs. The Israelis apparently discovered that a contractor to the National Security Agency (NSA), who had improperly taken classified documents home and stored them on his home computer that used Kaspersky's antivirus software, had his data compromised by these Russian hackers. This event reportedly occurred more than two years ago.[50]

Kaspersky Payments to Lt. Gen. (ret.) Michael Flynn

There are also other reasons that Kaspersky Lab has found itself a focus of attention recently. In October 2015, the U.S. subsidiary of Kaspersky Lab paid President Trump's former National Security Adviser Lt. Gen. (ret.) Michael Flynn $11,250 for a keynote speech at Kaspersky's Cybersecurity Forum in Washington, D.C.[51] Kaspersky Lab has said it was open about these

---

[46] "DHS Statement on the Issuance of Binding Operational Directive 17-01," Office of the Press Secretary, Department of Homeland Security (DHS), September 13, 2017, accessed here: https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01

[47] Mike Levine and Pierre Thomas, "Officials fear Russia could try to target US through popular software firm under FBI scrutiny," *ABC News*, May 9, 2017, accessed here: http://abcnews.go.com/US/officials-fear-russia-target-us-popular-software-firm/story?id=47295729

[48] "US intelligence chiefs have doubts about cybersecurity firm over its Russian roots," *The Guardian*, May 11, 2017, accessed here: https://www.theguardian.com/us-news/2017/may/11/kaspersky-labs-cybersecurity-us-senate-intelligence

[49] Mike Levine, "FBI interviews employees of Russian software firm raising security concerns in US: Source," *ABC News*, June 28, 2017, accessed here: http://abcnews.go.com/US/source-fbi-interviews-employees-russian-software-firm-raising/story?id=48328074

[50] Nicole Perlroth and Shane Harris, "How Israel Caught Russian Hackers Scouring the World for U.S. Secrets," *New York Times*, October 10, 2017, accessed here: https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html

[51] See: Taylor Hatmaker, "Kaspersky Lab paid former national security adviser more than $10,000," *Techcrunch*, March 16, 2017, accessed here: https://techcrunch.com/2017/03/16/kaspersky-michael-flynn/; Adam Goldman and Michael Schwirtz, "Michael Flynn Was Paid by Russian-Linked Firms, Letter Shows," *New York Times*, March 16, 2017, accessed here: https://www.nytimes.com/2017/03/16/us/politics/michael-flynn-russia-paid-trip.html; "Russian Tech Firm Confirms Payment to Former Trump Advisor Michael Flynn," *The Moscow Times*, March 17, 2017, accessed here: https://themoscowtimes.com/news/russias-kaspersky-labs-confirms-payment-to-former-trump-advisor-michael-flynn-57463

payments to Flynn and there was nothing to hide.[52] Flynn, who appears to be a focus of Independent Counsel Robert Mueller's investigation, resigned as National Security Adviser in February 2017 due to his lack of candor regarding his communication with Russian officials during the 2016 U.S. Presidential campaign.[53]

Hacking the U.S. Election Infrastructure

The U.S. intelligence community has been concerned about ties between Kaspersky Lab and Russian intelligence services for many years. However, they have not tied any publicly available information about Kaspersky Lab to the 2016 elections or to Russia's soft cyber influence campaign against the U.S. Despite that, Senator Amy Klobuchar (D-Minn.) has recently written at least two letters to the Department of Homeland Security regarding the potential use of

Kaspersky Lab software in the US election infrastructure.[54] The letters offered no evidence that Kaspersky Lab software was being used by election jurisdictions around the country, but the DHS directive issued last September that directs federal agencies to remove Kaspersky Lab software and products from their networks, does not apply to the hundreds of local, county and state voting jurisdictions that use a wide array of different information technologies to log votes at the ballot box and to maintain voter registration databases.

It is not surprising that concerns have been voiced regarding potential risks posed by Kaspersky Lab products, particularly in the US election infrastructure, given what the U.S. intelligence community has released publicly regarding their own assessment of Russia's wide-ranging influence campaign against the United States during the 2016 Presidential Election. The U.S. intelligence community assessment (ICA) determined that "Russian intelligence accessed

[52] Luke Harding, Stephanie Kirchgaessner and Nick Hopkins, "Michael Flynn: new evidence spy chiefs had concerns about Russian ties," *The Guardian*, June 30, 2017, accessed here: https://www.theguardian.com/us-news/2017/mar/31/michael-flynn-new-evidence-spy-chiefs-had-concerns-about-russian-ties

[53] Maggie Haberman, Matthew Rosenberg, Matt Apuzzo and Glenn Thrush, "Michael Flynn Resigns as National Security Adviser," New York Times, February 13, 2017, accessed here: https://www.nytimes.com/2017/02/13/us/politics/donald-trump-national-security-adviser-michael-flynn.html

[54] Adam Mazmanian, "Senator wants Kaspersky out of U.S. voting systems," Federal Computer Week, October 13, 2017, accessed here: https://fcw.com/articles/2017/10/13/klochubar-kaspersky-dhs-voting.aspx; and "Klobuchar Urges Department of Homeland Security to Ensure Election Systems are Free of Kaspersky Software," Press Release, Office of Senator Klobuchar, October 12, 2017, accessed here: https://www.klobuchar.senate.gov/public/index.cfm/2017/10/klobuchar-urges-department-of-homeland-security-to-ensure-election-systems-are-free-of-kaspersky-software

elements of multiple state or local electoral boards. Since early 2014, Russian intelligence has researched US electoral processes and related technology and equipment," the report concluded.[55] The ICA found that Russian intelligence directed cyberattacks against multiple U.S. targets associated with the 2016 elections. "In July 2015, Russian intelligence gained access to Democratic National Committee (DNC) networks and maintained that access until at least June 2016," the ICA said. By March 2016 the Russian military's main intelligence directorate, known as the GRU, "began cyber operations aimed at the US election" and by May 2016 had "exfiltrated large volumes of data from the DNC." This material, including e-mails, were released to third parties, including Guccifer 2.0, DCLeaks.com, and WikiLeaks, and then made public. Further, the ICA found that "Russia collected on some Republican-affiliated targets but did not conduct a comparable disclosure campaign."[56]

The U.S. election process is a decentralized labyrinth. It is composed of an estimated 10,000 separate local, county and state voting jurisdictions. On one hand this makes a potential cyberattack against the entire voting infrastructure difficult, but it also means that there is no centralized federal government oversight of the entire election process or the information technology products each local voting jurisdiction may use. As a result, hackers may seek to launch an attack against the weakest link in the system. However, the impact such attacks could have on the outcome of a nationwide election is incredibly difficult to predict, even for a sophisticated hacker. Nevertheless, it can lead to mistrust of the election process and undermine the public's trust in the potential election outcome and results. That alone, could be quantified as success for a determined adversary who seeks to discredit our democratic institutions and electoral process.

In January 2017, realizing the potential cyber risks to our election infrastructure and the reality that this infrastructure could be a fruitful target for a variety of foreign adversaries, the Department of Homeland Security (DHS) designated the U.S. election infrastructure as critical infrastructure. This designation will help DHS share sensitive cyber intelligence information with local and state election officials, and will provide greater access to potential security resources as well.[57] "Now more than ever, it is important that we offer our assistance to state and local election officials in the cybersecurity of their systems," then Secretary of Homeland Security Jeh Johnson said in statement on January 6, 2017, announcing the decision. "Election infrastructure is vital to our national interests, and cyber attacks on this country are becoming more sophisticated, and bad cyber actors – ranging from nation states, cyber criminals and hacktivists – are becoming more sophisticated and dangerous," he said.[58] This designation was

[55] "U.S. Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections," Office of the Director of National Intelligence, ICA 2017-01D, January 6, 2017, accessed here: https://www.dni.gov/files/documents/ICA_2017_01.pdf

[56] "U.S. Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections," Office of the Director of National Intelligence, ICA 2017-01D, January 6, 2017, accessed here: https://www.dni.gov/files/documents/ICA_2017_01.pdf

[57] See: "Elections as Critical Infrastructure: Background," U.S Election Assistance Commission, (Undated), accessed here: https://www.eac.gov/assets/1/6/CI_Overview_EAC.pdf; and "Starting Point: U.S. Election Systems as Critical Infrastructure," U.S Election Assistance Commission, (Undated), accessed here: https://www.eac.gov/assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf.

[58] Statement by Secretary of Homeland Security Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector, January 6, 2017, Office of the Press Secretary, Department of Homeland Security

later affirmed by President Trump's former Homeland Security Secretary John Kelly, now the President's White House Chief of Staff.[59]

In June 2017 the online magazine *The Intercept* disclosed a leaked top-secret document produced by the National Security Agency (NSA) that detailed some of the revelations regarding Russia's attempts to hack into U.S. voting-related systems. The documents, posted on-line, show that Russian hackers attempted to obtain the credentials of employees at VR Systems, a Florida-based firm that sells voter registration related computer gear to polling places in eight states, including California, Florida, Illinois, Indiana, New York, North Carolina, Virginia and West Virginia.[60] But the NSA analysis said it was unknown if the Russian hackers tied to a unit of Russia's military intelligence agency, known as the GRU, succeeded in its efforts to compromise VR Systems or to acquire any election related data.

In September 2017, the *New York Times* reported that hackers breached at least two other companies that provide election services well ahead of the 2016 Presidential election. The story also indicated that on election day in November 2016 in Durham, North Carolina, there were an unusually high number of mishaps with voters being told they were ineligible to vote when they were not and some being told they had already cast ballots earlier in the day, which was false. It is unclear what triggered this confusion and election day chaos in Durham, but the local election precinct uses VR Systems' software for its voter registration rolls.[61]

Later that same month, DHS notified 21 states that Russian hackers had been identified scanning their election systems in the run-up to the 2016 Presidential election. It was reported that there was no evidence of actual penetration of these networks or tampering with voter related data. Still, many of the states were understandably frustrated that it took DHS nearly one year to provide that information to these states. In addition, DHS later notified two of the 21 states, California and Wisconsin, that while those state's computer systems were scanned, the systems DHS identified in those states were not actually tied to the election infrastructure as DHS first indicated. North Carolina was not on the list of the twenty one states notified of these scans by DHS, according to a list of the targeted state's by the *Associate Press*.[62]

(DHS), accessed here: https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

[59] "Starting Point: U.S. Election Systems as Critical Infrastructure," U.S Election Assistance Commission, (Undated), accessed here: https://www.eac.gov/assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf.

[60] Matthew Cole, Richard Esposito, Sam Biddle and Ryan Grim, "Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election," *The Intercept*, June 5, 2017, accessed here: https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/

[61] Nicole Perlroth, Michael Wines and Matthew Rosenberg, "Russian Election Hacking Efforts, Wider Than Previously Known, Draw Little Scrutiny," *New York Times*, September 1, 2017, accessed here: https://www.nytimes.com/2017/09/01/us/politics/russia-election-hacking.html

[62] See: Geoff Mulvihill and Jake Pearson, "Federal government notifies 21 states of election hacking," *Associated Press*, September 23, 2017, accessed here https://www.washingtontimes.com/news/2017/sep/22/federal-government-notifies-21-states-of-election-/; and Christina A. Cassidy and Chad Day, "Homeland Security Clarifying State Election Hacking Attempts," *Associated Press*, September 27, 2017, accessed here: http://www.chicagotribune.com/news/sns-bc-us--russian-hacking-states-20170927-story.html

It is important to understand that the Russian soft cyber influence campaign was clearly not just about potentially manipulating the physical votes at the ballot box. It was about polluting the cognitive decisions made by voters at the ballot box by inundating the public with false news, half-truths and disinformation that sought to create chaos and confusion during the 2016 US Presidential Election in order to undermine the democratic electoral process. In large part, they succeeded in those endeavors. James Clapper, the former Director of National Intelligence told POLITICO in an interview in October 2017, "The Russians succeeded, I believe, beyond their wildest expectations."[63]

During testimony before Congress in June 2017, the former Director of the Federal Bureau of Investigation (FBI) James Comey, described the Russian efforts to influence the American public and undermine our democracy this way:

> We have this big messy wonderful country where we fight with each other all the time. But nobody tells us what to think, what to fight about, what to vote for except other Americans. And that's wonderful and often painful. But we're talking about a foreign government that using technical intrusion, lots of other methods tried to shape the way we think, we vote, we act. That is a big deal. And people need to recognize it. It's not about Republicans or Democrats. They're coming after America, which I hope we all love equally. They want to undermine our credibility in the face the world. They think that this great experiment of ours is a threat to them. So they're going to try to run it down and dirty it up as much as possible. That's what this is about and they will be back. Because we remain — as difficult as we can be with each other, we remain that shining city on the hill. And they don't like it."[64]

[63] Susan B. Glasser, "'The Russians Have Succeeded Beyond Their Wildest Expectations,'" *POLITICO Magazine*, October 30, 2017, accessed here: https://www.politico.com/magazine/story/2017/10/30/james-clapper-russia-global-politico-trump-215761

[64] "Full text: James Comey testimony transcript on Trump and Russia," A transcript of former FBI Director James Comey's testimony before the Senate Intelligence Committee on June 8, 2017, *POLITICO*, accessed here: https://www.politico.com/story/2017/06/08/full-text-james-comey-trump-russia-testimony-239295

Digital Trojan Horses

The global information infrastructure, created and expanded by the innovation of largely American companies, has brought tremendous positive elements to people, industries, governments and communities around the world. However, in many ways, the Russian interference in recent elections in both the United States and other western democracies, has shown us that the innovative social media tools that are now the digital pit-stops along this information superhighway can be manipulated to be digital trojan horses of undue and often covert influence aimed at disrupting, disinforming, and dividing the American public.

The Soviet Union used multiple methods to deceive the United States in the past, often to conceal or obscure their military weaknesses. In 1965, during the Cold War the Soviet Union marched two huge strategic missiles, known as the GR-1, an acronym for Global Missile, across Moscow's Red Square in a military parade. The sight of the missiles reportedly led NATO and American officials to scramble to attempt to discover ways to defend against the monstrous missiles. This event apparently led the U.S. to spend millions on a missile defense system. But there was only one problem. The Soviets had already abandoned efforts to develop the GR-1 long before it was paraded in front of Western officials, and other missiles in the parade were dummies too. The Soviet intent was to scare their adversaries, according to a 1998 article in the Russian language magazine *Vlast* (*Power*).[65] It worked. It was a classic example of Reflexive Control, suggests Timothy Thomas.

The tools the Russians have deployed to engage in reflexive control operations today have changed, but the tactics remain very much the same. They have replaced fake missiles with fake social media sites. In September 2017, the *New York Times* broke a story that detailed how fake Facebook pages were created by individuals believed to be linked to Russian military intelligence.[66] The title of the article, ***"The Fake Americans Russia Created to Influence the Election."*** Russian operatives apparently hijacked a photograph of a Brazilian native and turned

[65] See: "Russia Paraded Dummy Missiles," *The Independent*, November 18, 1998, accessed here: http://www.independent.co.uk/news/moscow-paraded-dummy-missiles-1185682.html; and "Flashback: Fake missiles in Soviet parade?" *Fox News*, April 17, 2017, accessed here: http://video.foxnews.com/v/5401274109001/?#sp=show-clips

[66] See: Scott Shane, "The Fake Americans Russia Created to Influence the Election," *New York Times*, September 7. 2017, accessed here: https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html and Scott Shane, "Mystery of Russian Fake on Facebook Solved, by a Brazilian," *New York Times*, September 13, 2017, accessed here: https://www.nytimes.com/2017/09/13/us/politics/russia-facebook-election.html

him into an American they named Melvin Redick and placed his artificial persona in Harrisburg, Pennsylvania. Not only did the fake Mr. Redick post multiple derogatory messages about Hillary Clinton, but he pointed his followers to DCLeaks.com, a website that became a vehicle for releasing hacked e-mails. According to the U.S. ICA on the Russian influence campaign, the DCLeaks website was used as a vehicle of the Russian military intelligence directorate, known as the G.R.U., to release hacked DNC e-mails related to the 2016 Presidential Election.[67] The incident, detailed in the *New York Times* story shows the sophistication and extremes to which those reportedly linked to the Russian intelligence services went in order to disrupt the 2016 Presidential Elections in a wide-ranging and aggressive deceptive influence campaign.

Stoking Fears & Sowing Discontent

In October 2017, *CNN* reported that a group called Black Fist was linked to a Russian troll farm that apparently generated thousands of fake Facebook ads and had paid personal trainers in New York, Florida and other states to run self-defense classes for African Americans.[68] All of this was done, according to several news stories, in an attempt to stoke fear and collect information on individuals who might be susceptible to pro-Russian propaganda. It was believed the operation was linked to the pro-Russian Internet Research Agency.[69] The fake group, Black Fist, was reportedly established in January 2017, two months after the 2016 US Presidential election, and used the social media sites Facebook, Instagram, Eventbrite and MeetUp to lure African Americans into self-defense classes that the stealthy organizers appear to have tried to use for their own propaganda purposes. The endeavor was sophisticated. The organizers paid one self-defense instructor in New York through Google Wallet and later PayPal. But when the *CNN* reporters tracked down the information from the PayPal account it led them to a woman in North Carolina who had never heard of the Black Fist group. What's most interesting is that the Black

[67] "U.S. Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections," Office of the Director of National Intelligence, ICA 2017-01D, January 6, 2017, accessed here: https://www.dni.gov/files/documents/ICA_2017_01.pdf

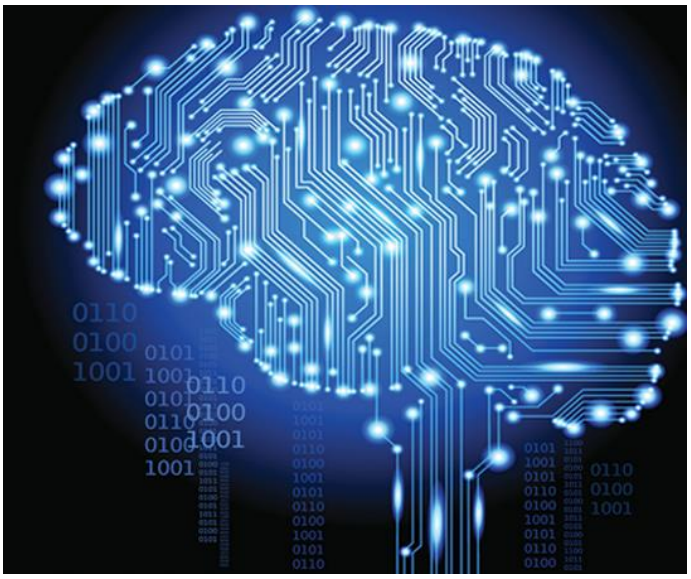
[68] See: Donie O'Sullivan, Drew Griffin and Curt Devine, "In attempt to sow fear, Russian trolls paid for self-defense classes for African Americans," *CNN Money*, October 18, 2017, accessed here: http://money.cnn.com/2017/10/18/media/black-fist-russia-self-defense-classes/index.html and Maya Kosoff, "The Russian Troll Farm That Weaponized Facebook Had American Boots on the Ground," *Vanity Fair*, October 18, 2017, accessed here: https://www.vanityfair.com/news/2017/10/the-russian-troll-farm-that-weaponized-facebook-had-american-boots-on-the-ground

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

Fist group was created months after the 2016 Presidential Election and appears to show that Russia's efforts to disrupt American society are continuing unabated.

Computer Code & Human Thought Code: Impact & Influence

A critical component in understanding Russia's holistic view of information warfare is that they do not limit their vision to simply obtaining bits and bytes of digital data or computer code. The real target for Russian influence operatives is the human mind. They seek to influence our behaviors and actions. Ironically, we have provided them with the means to do so.



Several computer and social scientists at the RAND Corporation have begun to probe the Russian influence campaign through the lens of behavioral social science and what one RAND researcher terms "cognitive security." At a hearing before the Subcommittee on Cybersecurity of the Senate Armed Services Committee last April, Rand Waltzman, provided testimony that he titled: "The Weaponization of Information: The Need for Cognitive Security." He wrote, "The massive explosion of behavioral data made available by the advent of social media has empowered researchers to make significant advances in our understanding of the dynamics of large groups online. However, as this field of research expands, opportunities multiply to use this understanding to forge powerful new techniques to shape the behavior and beliefs of people globally. These techniques can be tested and refined through the data-rich online spaces of platforms like Twitter, Facebook and, looking to the social multimedia future, Snapchat," he wrote. He ended with a pitch for the development of a Center for Cognitive Security that would bring together experts in the fields of cognitive science, computer science, engineering, social science, psychology and others to identify and understand influence campaigns waged against us by foreign adversaries and to develop methods to defend against them.[70]

Two other social scientists at RAND, Christopher Paul and Miriam Matthews, recently published a study based on an extensive literature review on influence and persuasion as well as experimental research from the field of psychology. They published a report last year titled: "The Russian "Firehose of Falsehood" Propaganda Model."[71] They made several telling observations. Russian use of propaganda has a strong foundation in psychology. This is not surprising, given

[70] Rand Waltzman, "The Weaponization of Information: The Need for Cognitive Security," Written Testimony at a hearing titled: *Cyber-enabled Information Operations* before the Senate Armed Services Committee, Subcommittee on Cybersecurity, April 27, 2017, accessed here: https://www.armed-services.senate.gov/imo/media/doc/Waltzman_04-27-17.pdf

[71] Christopher Paul and Miriam Matthews, "The Russian "Firehose of Falsehood" Propaganda Model," *Perspective*, RAND Corporation, 2016, accessed here: https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf

the fact that Vladimir Lefebvre, the father of Reflexive Control Theory, had his academic roots in psychology. Russian propaganda, the RAND researchers found, had four distinctive attributes. It was 1) High-volume and multichannel; 2) Rapid, continuous, and repetitive; 3) Lacks commitment to objective reality; 4) Lacks commitment to consistency.

"Experimental research in psychology suggests that the features of the contemporary Russian propaganda model have the potential to be highly effective," the researchers concluded. The authors' literature review showed that, "Multiple sources are more persuasive than a single source," "Repeated exposure to a statement has been shown to increase its acceptance as true," and first impressions are resilient and individuals are often more likely to accept their first impression of an issue. As a result, since Russian cyber influence operatives are not beholden to facts and can rapidly disseminate information without the added inconvenience of verifying claims or checking facts, they can respond rapidly and repetitively to news stories and events giving their false narratives or deceptive storylines an upper hand. "[D]on't expect to counter the firehose of falsehood with the squirt gun of truth," write the authors. Instead, they suggest, "It may be more productive to highlight the ways in which Russian propagandists attempt to manipulate audiences, rather than fighting the specific manipulations."[72]

Countering Soft Cyber Influence Operations

A fundamental tenet of the United States has always been the ability of an open, free and diverse press to publish freely, widely and without constraint. In the past, established media organizations have had their own internal checks and balances, including teams of fact-checkers.

These organization dedicated resources to verify and clarify the factual basis of claims before they were published or aired through their media outlets.

The digital dawn of the world wide web enabled the expansion of publication opportunities for anyone with an Internet connection. However, that power has been magnified over the past decade with the development of various social media platforms allowing individual users to disseminate information to a large and wide-ranging global audience. Much of the information disseminated across these platforms does not have any checks or balances regarding the factual basis of the content of the information that is disseminated. In some cases, the clear intent is to knowingly push false news stories forward.

[72] Ibid.

Fake news is not a new phenomenon, but the ease, access, and ability to generate and distribute knowingly false information is undeniably greater today than it has ever been. Nation-states, organizations, and single individuals now have the ability to reach literally millions of social media followers in an instant with a few taps on the keyboard. The intentions of these actors may be difficult to discern, but the effects and potentially unintended consequences of these actions can be both wide-ranging and severe.

The potential social chaos and political consequences that false news stories can cause has become a global threat. In 2013, the World Economic Forum's Global Risks report listed massive digital misinformation alongside terrorism, cyber-attacks, and the failure of global governance as a serious threat that "could enable 'digital wildfires' to wreak havoc in the real world." The report referenced some technical solutions being investigated by researchers and computer developers, "that aim to help people assess the credibility of information and sources circulating online. It is possible to imagine," the report said, "the development of more broad and sophisticated automated flags for disputed information, which could become as ubiquitous as programs that protect Internet users against spam and malware."[73]

Over the past few years many efforts have been launched to develop the tools and technologies to help identify false news stories and inform the public about them. Many of these new projects are coordinated efforts by media outlets, academic journalism programs, social scientists and technology companies attempting to identify technical methods to identify fake news related stories, identify the origins of the stories, and forewarn the public about their lack of veracity. What follows below is an incomplete listing of some of these emerging efforts.

Some fact-checking organizations have been developed specifically to counter Russia's disinformation and soft cyber influence campaigns. Stopfake.org, for instance, was launched in March 2014 by teachers and students at the Mohyla School of Journalism at the National University in Kiev, Ukraine in an effort to fight "untruthful information about events in Ukraine" and to identify and refute Russian propaganda and methods of influence regarding Russia's annexation of Crimea.[74]

The Center for European Policy Analysis (CEPA), a non-profit policy institute dedicated to the study of Central and Eastern Europe with offices in Washington, D.C. and Warsaw, Poland, has developed an "innovative, program to monitor, collate, analyze, rebut and expose Russian disinformation" campaigns in Central and Eastern European countries. According to their website the program "brings together leading journalists, activists and media analysts from Europe's frontline states and utilizes their expertise to develop an analytical toolkit for

[73] Global Risks 2013, Eighth Edition, World Economic Forum, accessed here: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf
[74] See Stopfake.org, accessed here: https://www.stopfake.org/

effectively dealing with Russian disinformation at the institutional, strategic and conceptual levels."[75]

Columbia University's Tow Center for Digital Journalism, for instance, has launched "Emergent," described as "a real-time rumor tracker … that focuses on how unverified information and rumor are reported in the media." Emergent's aim is "to develop best practices for debunking misinformation."[76]

Researchers at the Indiana University's Network Science Institute (IUNI) and the School of Informatics and Computing's Center for Complex Networks and Systems Research (CNetS) are also working on a tool called Hoaxy to enable the reconstruction of how false news stories, rumors, conspiracy theories, and hoaxes are disseminated across the Internet. "Hoaxy will allow researchers, journalists, and the general public to study the factors that affect the success and mitigation of massive digital misinformation," the researchers write. "Hoaxy visualizes the spread of claims and related fact checking online," according to its web-site. "A claim may be a fake news article, hoax, rumor, conspiracy theory, satire, or even an accurate report. Anyone can use Hoaxy to explore how claims spread across social media."[77]

Tech companies that maintain social media platforms, such as Facebook, Twitter, Google, and others have also begun to address these issues. More than 30 news organizations and social media technology companies created an organization called First Draft News that provides "practical and ethical guidance in how to find, verify and publish content sourced from the social web." First Draft News includes academic research partners from more than three dozen universities and was created so these organizations could share best practices on how to verify true news stories and stop the spread of fake ones.[78]

CrossCheck is a project developed by First Draft and the Google News Lab that was formed to help identify and "false, misleading and confusing claims that circulated online in the ten weeks leading up to the French Presidential election" held in the spring of 2017. The project brought together 37 newsroom partners in France and the United Kingdom with the aim of providing the "public with the necessary information to form their own conclusions about the information they receive."[79]

FactCheck.Org, a project of the Annenberg Public Policy Center, has

[75] See CEPA's StratCom Program, accessed here: http://www.infowar.cepa.org/index/?lang_id=4
[76] See Emergent, accessed here: http://www.emergent.info/about
[77] See Hoaxy, accessed here: https://hoaxy.iuni.iu.edu/faq.html
[78] See First Draft News, accessed here: https://firstdraftnews.com/
[79] CrossCheck: A collaborative journalism project, accessed here: https://crosscheck.firstdraftnews.com/france-en/

published a guide on "How to Spot Fake News" and also released a short video called "Spotting Fake News" that summarizes this guide.[80]

In September 2017, the John S. and James L. Knight Foundation, the Facebook Journalism Project and the Craig Newmark Foundation announced they are awarding $1.2 million in grants to the Duke University Reporters' Lab to automate fact-checking. During the two-year long project "computer scientists and journalism faculty from Duke, the University of Texas at Arlington and Cal Poly-San Luis Obispo will build a variety of new tools and apps. Some will help journalists with time-consuming reporting tasks, such as mining transcripts, media streams and social feeds for the most important factual claims," according to the press release. The new project will be called the Duke Tech & Check Cooperative.[81]

Free speech is one of the most important and fundamental principles of our Constitution. However, the advent of fake news and the implications and impact it can have on our democracy, security, and society is a new reality. Understanding the labyrinth of intentionally misleading and false news stories that have begun to permeate the world wide web, and that can have a profound impact on the public and U.S. government policymakers alike, is critically important. Developing the scientific methods and technical tools to flag these false stories and inform the public about them will help protect our democratic institutions from active soft cyber influence operations whether launched by Russia or any other entity.

The Science Committee can play an important role in holding public hearings on how to better protect our election infrastructure against potential cyberattacks and in examining new and emerging technologies that can help to identify foreign influence operations that seek to disseminate disinformation, distorted facts and fake news with the intent of undermining our democracy and democratic institutions. Ignoring these past actions by Russia or dismissing their impact on our government and society will not make them go away. They will continue. This is a new reality and the Science Committee can take an important leading role in evaluating how the U.S. government and the overall scientific community and technical experts can respond appropriately. We cannot predict who the next target of these influence operations may be, but regardless of who our foreign or other adversaries attack next, the repercussions can impact us all.

[80] See: Eugene Kiely and Lori Robertson, "How to Spot Take News," FactCheck.Org, November 18, 2016, accessed here: http://www.factcheck.org/2016/11/how-to-spot-fake-news/ and Spotting Fake News, produced by FactCheck.Org, posted on December 8, 2016, accessed here: https://www.youtube.com/watch?v=AkwWcHekMdo&feature=youtu.be

[81] Bill Adair, "Knight Foundation, Facebook and Craig Newmark provide funding to launch Duke Tech & Check Cooperative," Press Release, Duke Reporters' Lab, September 25, 2017, accessed here: https://reporterslab.org/category/fact-checking/#article-1788