How Russia hacks our democracy

Medium (https://medium.com/short-bytes/how-russia-hacks-our-democracy-2c5460596bc3) · by Matt Chessen

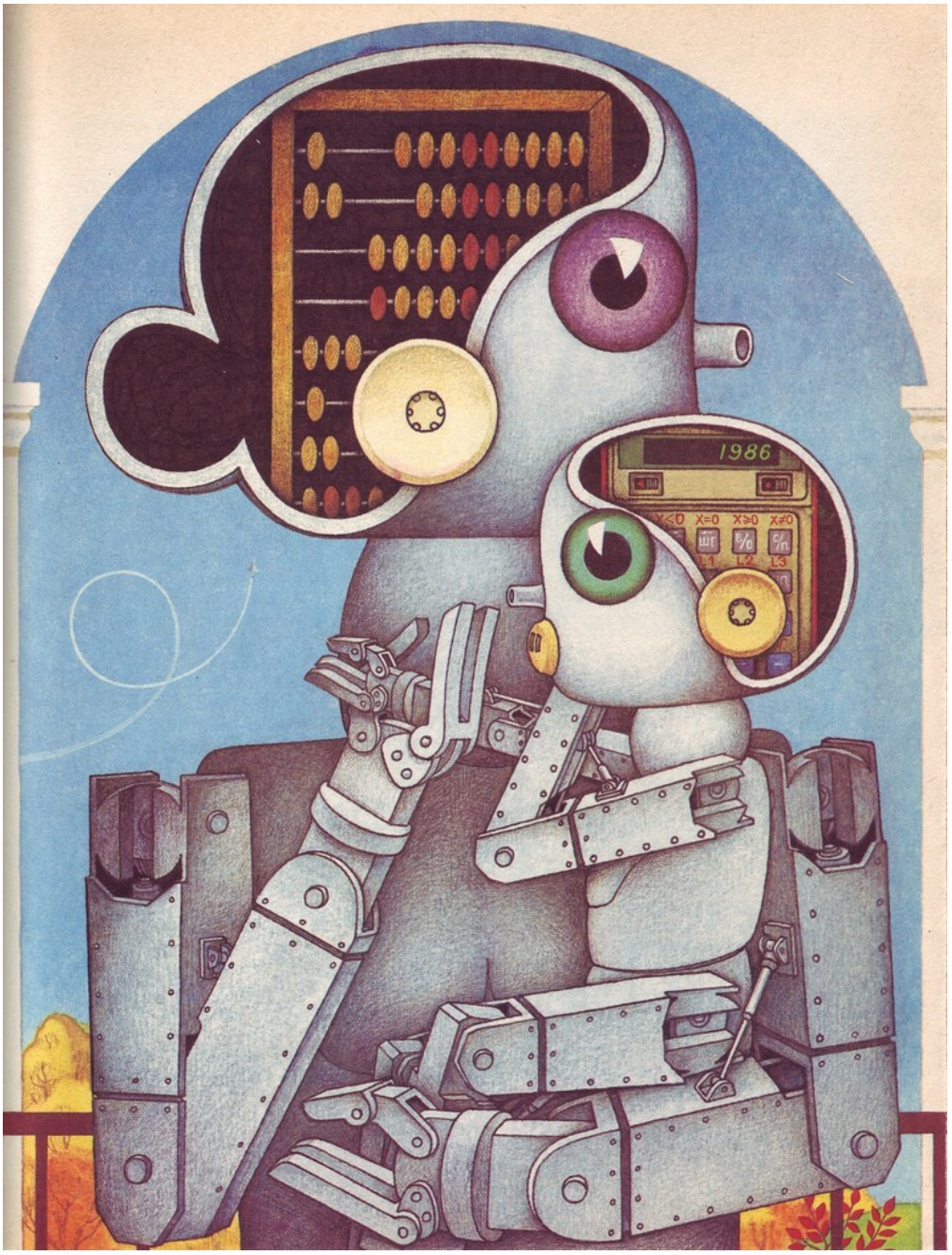

Image courtesy of E. Benyaminson (https://www.flickr.com/photos/ajourneyroundmyskull/4205226788)

I. Introduction

Russia is engaging in hybrid warfare with 'the West' (broadly defined as the liberal democracies that make up NATO) and its allies. This hybrid warfare occasionally involves kinetic action—such as the 2008 Russian invasion of Georgia and the 2014 intervention in Ukraine and annexation of Crimea—but most of the activity is nonviolent information warfare. The Kremlin weaponizes money, culture and information in an effort to shatter enemy communications, demoralize its enemies and disrupt enemy command structures (http://www.interpretermag.com/the-menace-of-unreality-how-the-kremlin-weaponizes-information-culture-and-money/%20).

During previous global conflicts, these objectives were often achieved through violent means. However, the explosion in global communications technology, the Internet and social media provided Russia with the technological means to accomplish these objectives without direct confrontation. Information warfare capitalizes on the West's vulnerabilities by weaponizing information but minimizes riskier conflicts in military, economic and diplomatic realms where Russia faces asymmetric disadvantages.

The rise of the Internet and social media were key technological enablers of this information warfare model. This paper will explore the contrasts between how the Soviet Union ran disinformation operations, and how Russia now runs similar operations with much greater efficacy due to technology. This discussion will uncover the nature of science and technology power, and how this power will grow more important over the next ~20 years. It concludes with recommendations for policy-makers about how to mitigate similar asymmetric uses of science and technology power by adversaries in the future.

II. Russian disinformation: from active measures to the rise of the Internet

Russia has a long history of utilizing disinformation as a tool for national power, dating back to the Soviet era. The USSR used 'aktivniye meropriyatiye' (active measures) to influence world events by manipulating society, politics and media. As retired KGB General Oleg Kalugin defined it, active measures were designed: "to drive wedges in the Western community alliances of all sorts, particularly NATO, to sow discord among allies, to weaken the United States in the eyes of the people in Europe, Asia, Africa, Latin America, and thus to prepare ground in case the war really occurs (http://www.thedailybeast.com/articles/2016/07/26/putin-s-wicked-leaks-didn-t-start-with-the-dnc.html)."

Active measures was a multi-channel approach to conflict using tools ranging from subtle disinformation to outright political violence. A key element of active measures was information warfare: the use of information and communication tools to gain an advantage over opponents. Modern information warfare can include elements like hacking and electronic warfare, but this analysis focuses on efforts to hack the human mind—propaganda and disinformation. The Soviet Union used these methods against the United States repeatedly throughout the Cold War, with varying effect.

Dezinformatsiya (disinformation) operations spread what we now refer to as fake news in an effort to manipulate adversaries, defame them, generate internal social disharmony, and undermine confidence in government and institutions (http://www.interpretermag.com/the-menace-of-unreality-how-the-kremlin-weaponizes-information-culture-and-money/%20). Two of the most famous of these operations were the KGBs efforts to cultivate the belief that the CIA assassinated President Kennedy, and Operation Infektion—the Soviet Union's attempt to blame the CIA for the creation of the AIDS virus.

The Soviet Union used a multi-channel, multi-media approach to these efforts. The KGB would would pay academics, journalists and other 'experts' to publish articles promoting the disinformation. Then Russia would follow up with a flood of articles and media citing those independent foreign investigative journalists and researchers. Occasionally these subtle disinformation efforts were complemented by more overt activities like distributing leaflets in communities, promoting demonstrations or riots, and the occasional threatened or murdered journalist or politician. Frequently, disinformation efforts were coordinated with campaigns to support guerrilla insurgent movements, schemes to establish puppet governments along Russia's periphery and political assassinations of international leaders. The disinformation operations supported military, intelligence and diplomatic operations.

However, disinformation efforts were only mildly successful due to the limitations inherent in the information and communication landscape. On one hand, many developing countries lacked widespread access to information and communication technologies (ICTs), and indigenous media sources were lacking, so their citizens were vulnerable to disinformation. But wealthier countries had rich media environments, strong institutions, a robust environment of investigative journalism and fact checking, and an inherent suspicion and distrust of Soviet media and developing country sources. ICTs at that time were local, not global, and their reach was constrained compared to today. The Soviet Union faced significant difficulties in getting its messages to a critical mass of audiences

in Western countries, and those messages which did get through frequently weren't credible or were only believed by fringe elements of society. During the Cold War these disinformation efforts did not have a strategic effect on opposition communications, morale or command structure.

The dramatic expansion of ICTs over the last 20 years completely transformed the context in which information warfare would be contested. Information warfare is about using information and communication as a tool of conflict. The emergence of the Internet and associated technologies like the World Wide Web, social media, discussion boards, comment sections and the like was a tectonic technological shift in the domain where information and communication operations would occur.

During the Cold War, the dominant ICTs were newspapers, magazines, journals, television, and radio. These all had physical limitations that constrained their effectiveness. The emergence of cyberspace bypassed those physical limitations to engage the entire world in a contest for information supremacy.

III. The power of modern information and communication technologies for disinformation

Russia didn't invent modern ICTs and its science and technology (sci-tech) power is modest compared to the West. However, while it didn't invent these technologies, it did create both a strategy and a doctrine for using our own technology against us. Russia uses ICTs to exploit weaknesses in the liberal democratic system the West is based on. Russia uses the openness of our societies, and our commitment to free speech as weapons by pushing disinformation and propaganda out through ICT channels that provide new capabilities and enhance old tools.

A comparison of Soviet era disinformation efforts and the far more successful efforts using modern ICTs reveals how information is weaponized and the key attributes of sci-tech power that facilitate weaponization. For illustrative purposes, these attributes will be evaluated using terminology typically applied to weapons systems.

Range: The Soviets had difficulty deploying weaponized information directly into Western countries because those countries already had rich, insular media environments that were disconnected from Russia. Placing Russian stories in American media, leafletting, political agitation and the like typically required agents in the United States. This was expensive and inherently risky. The Internet

flattened all barriers to global communication. Governments and citizens from any country on the globe can communicate directly with institutions or individuals anywhere through ICTs. Now, Russia can deliver its disinformation directly to individual citizens within adversary nations, without its operatives ever leaving the homeland.

Speed: Soviet era disinformation campaigns were long operations that took years to play out. Operation Infektion was initiated in 1983 through an anonymous letter to a Soviet-Indian newspaper that had been established in 1962. The false story about the CIA creating the AIDS virus (https://en.wikipedia.org/wiki/Operation_INFEKTION#Story_genesis_and_progression%20) began spreading in 1985 and was most active from 1987 to 1988. Disinformation operations took time to build a broad base of credibility. Now, computational propaganda utilizes machine-driven communication tools to constantly blast disinformation worldwide across a multitude of platforms. Operatives in Russia generate new fake news stories, websites and memes in a matter of hours, and use ICTs to spread them across the Internet at the speed of viral social media. Dumb bots are instructed to post content in response to pre-programmed triggers instantly, before news organizations or governments have an opportunity to respond to events. Bot networks work together to game algorithms (and human cognition) and promote disinformation content as trending news. Emerging artificial intelligence technologies will enhance this ability further, enabling machines to dynamically create persuasive conversations or content on the fly. AI tools won't just respond to events based on triggers, they will evolve the disinformation campaign as events unfold. Machines work at the speed of light, they never need rest, and they never take breaks. Humans can't compete with their speed.

Cost efficiency: Soviet disinformation campaigns required a worldwide network of spies housed overseas, utilizing bribery or leverage to convince academics, journalists and experts to promulgate the disinformation. Now, the infamous Russian Web Brigades are comprised of a few thousand young people, paid relatively low wages, using basic computer systems and Internet access to spread disinformation globally (https://www.nytimes.com/2015/06/07/magazine/the-agency.html). Russia Today (RT), a propaganda arm of the Russian government, does receive significant funding of $19 billion Rubles per year ($300 million USD), but this is money well spent. RT is an international news network in multiple languages, its technologists effectively game algorithms so its content appears at the top of

search results, RT's YouTube videos are extremely popular in media-scarce countries, and many people, (including many Americans) have no idea RT is a propaganda tool for the Russian government.

Irregular forces: Regular Soviet citizens had few, if any, real opportunities to help their country's information operations. Now, 'Patriotic Hackers' and organized crime groups frequently bolster Russian government online information operations, or conduct their own hacking or information without any government guidance. ICTs empower everyone with a computer and Internet access as a potential combatant, and similarly, anyone using ICTs is a potential casualty of war.

Rate of fire: Soviet era disinformation required a significant investment of time and resources, so the KGB had to be judicious in what campaigns it operationalized. Now, because computational propaganda via ICTs is so easy and cost effective, Russia can run dozens of campaigns simultaneously. Russian Web Brigades post massive amounts of content on social media daily. They expand on posts that are effective, discard the others, and initiate new campaigns all within the timeframe of a single Cold War era news cycle. Much of the quality isn't good, but it is cheap and fast, and in compressed news cycles, volume trumps quality. (The illusory truth effect (https://en.wikipedia.org/wiki/Illusory_truth_effect%20)and other psychological phenomena (http://www.state.gov/documents/organization/271028.pdf) demonstrate that people believe information after repeated exposure, regardless of the quality).

Stealth: Soviet disinformation campaigns were crafted with great care in order to hide the ultimate source of the stories. Disinformation sources were developed in foreign countries and then cited by Russian media only when the KGB could create the illusion of an emerging international consensus. If the story was traced back to Russian origins, years of careful work could be spoiled. Now, anyone can obtain social media accounts and websites anonymously and use them for disinformation. Many of these fake news sites emulate legitimate American news organizations and propagandist social media account profiles mimic normal Americans. (The psychological theory of implicit egotism (https://en.wikipedia.org/wiki/Implicit_egotism%20) explains that humans have an unconscious preference for things they associate with themselves. For a full description of psychological techniques, see Understanding the Psychology Behind Computational Propaganda in this report (https://www.state.gov/documents/organization/271028.pdf)). If a single site or account is exposed, the blowback is minor and it's easy to abandon them and

procure new ones. There is almost no capability for U.S. citizens and little capability for U.S. institutions to identify and attribute propaganda campaigns run over ICTs.

IV. ICTs, disinformation and the nature of science and technology power

Discussing ICT attributes in these terms reveals how Russia uses sci-tech power to weaponize information and dramatically enhance the effectiveness of disinformation operations. These are core attributes of sci-tech power—it can provide totally new capabilities or increase the effectiveness of existing tools or methods. However, new capabilities or increased effectiveness are not necessarily the only or best value propositions for sci-tech power. For example, simply building a new type of bomb or a bigger bomb doesn't necessarily mean it will be effective in conflict. The weapon has to help achieve some strategic objective and must be integrated into doctrine and existing systems. Additionally, opponents frequently make similar inventions and can steal your technology for their own use, leveling the playing field. Globalization, modern communications technologies, cyber-enabled theft of intellectual property, and the diffusion of science and technology talent across the world means innovations will rarely remain secret or available to only one nation for long.

The example of Russian use of ICTs for disinformation also reveals a less obvious attribute of sci-tech power—opponents can use your superior technology against you. Russia did not invent the Internet, the World Wide Web, social media, microchips or most of the other technologies they use for computational propaganda and disinformation. These were invented in the West and Russia now uses them against their inventors. Russia recognized that its strategic objectives could be accomplished through modern ICTs and it developed doctrines for using those innovations to further its goals. The West invented most of these technologies, but they didn't necessarily provide it an advantage in information warfare. In fact, because of the West's commitment to openness and freedom of speech, these technologies allowed an adversary unprecedented ability to attack U.S. citizens and institutions (Similarly, the 9/11 hijackers used a Western technology—the airliner—and Western openness—easy air travel—against its creators.).

This insight argues for less emphasis on pushing the boundaries of science and technology to develop new, game-changing technologies simply for invention's sake, because inventions won't necessarily serve strategic goals. Instead, it argues for more focus on how current technologies could be exploited for advantage, and more analysis of where technologies present new vulnerabilities.

In this discipline of strategic foresight, the West badly misjudged how ICTs would impact closed societies and how vulnerable it made their own citizens and institutions (Using the terminology of Stephen Rosen, the West focused on one strategic measure of effectiveness (ICT impacts on authoritarian governments) at the expense of an equally important one (vulnerabilities created by ICTs)). At the dawn of the 21st Century, the conventional wisdom was that the Internet and other ICTs would spell doom for authoritarian regimes. The theory held that ICTs would enable citizens in those regimes to access information, organize, expose the corruption and hypocrisies of their leaders, and undermine the iron first of dictatorship. One could argue the Arab Spring was a model example of this paradigm in action as citizens used social media and other modern ICTs to spread information on corruption, organize protests and facilitate the overthrow of several governments. However, the more sophisticated regimes in Russia and China recognized this existential threat and adapted to it with different strategies.

Russia took the disinformation route,(China chose an information control model, using the Great Firewall to limit access to information and actively suppressing dissent or distracting from it when it appeared) using ICTs to spread disinformation that eroded faith in institutions and the media. . It used ICTs to cultivate a multitude of dissenting voices to keep the opposition fragmented. It's disinformation eroded belief that objective truth even exists. The government filled this vacuum by creating an information environment that is equal parts entertainment, nationalistic identity-building, and authoritarian propaganda and disinformation, with small elements of violence amplified through the State's total control of the media. Citizens have access to outside information, but they've been effectively brainwashed into believing that all information is biased and the West is out to destroy Russia. This inoculates the Putin regime from the vulnerabilities presented by the Internet and other ICTs. It is an excellent example of how effective strategic analysis resulted in new doctrines that effectively defended Russia from a technology threat created by a superior sci-tech adversary.

Once Russia secured its own vulnerabilities, it looked outwards and turned ICTs on its creators. Whereas Russia's vulnerability was the possibility that open access to information might reveal regime excesses and facilitate a coordinated opposition, the West's vulnerability was its fundamental belief in free speech and the marketplace of ideas. The United States had additional vulnerabilities, including a cultural distrust of government, significant racial divisions, and a large and extremely heterogeneous population. Russia capitalized on these vulnerabilities, using fake news and computational propaganda to undermine faith in the media, government, and truth itself. It used these tools to exacerbate

Red-Blue divides, racial tensions, and class/economic differences to pit Americans against each other. Russia meddled in the U.S. election, seeking to divide America, erode confidence in our elections and undermine the credibility and legitimacy of both candidates, regardless of who won. These were Russia's tactical measures for exploiting technology to achieve its strategic goals: shattering enemy communications; demoralizing its enemies; and disrupting enemy command structures.

V. Russia effectively used sci-tech to overcome significant disadvantages

Russia utilizes sci-tech power to accomplish its strategic goals because it faces disadvantages in other areas of national power that are not vulnerable to asymmetric exploitation. Unlike sci-tech power, economic power can not be deployed asymmetrically. Economic power requires a strong, diverse domestic economy and robust international trade that Russia lacks. Russia's modest economy is primarily driven by petroleum products that are traded in dollars and subject to market forces outside its control. Russia tried to exploit its economic power against Europe from 2005–2010 by disrupting natural gas supplies, but this backfired as Europe responded by cultivating alternative suppliers. Russia can bully smaller economies like Ukraine that are dependent on Russian trade, but it is vulnerable to sanctions imposed by the larger economies of the West.

Russia also faces insurmountable military vulnerabilities because its economy can not support conventional forces to match the United States and NATO. Any direct conventional conflict would result in catastrophic losses that would leave Russia the unfavorable option of suing for peace, or the suicidal option of escalating a conventional conflict to a nuclear one. Therefore Russia is limited to using its military power in areas like Georgia, Crimea, Ukraine and Syria, where it isn't in direct confrontation with the West, and the scale of its involvement doesn't pass the threshold for NATO intervention. Whereas Russia can use ICTs to confront the West directly with lower risks, any direct military confrontation risks disastrous or apocalyptic outcomes.

Russia has limited ability to capitalize on diplomatic power. Effective diplomacy requires long-term partnerships, shared interests, influence and, occasionally, leverage. The dissolution of the Soviet Union saw Russia's realm of reliable partners shrink dramatically. In international forums, Russia frequently finds an ally in China on opposition to Western concepts ranging from the multistakeholder model of Internet governance to military interventions in authoritarian states. But it lacks an alliance of powerful friends. Russia does possess influence through its U.N. Security Council seat, but rather than an

affirmative power, the real influence is through its ability to veto U.N. resolutions. It can block initiatives, but it can't force them through. And while Russia has many skilled diplomats, diplomatic power doesn't reside in the people so much as it resides in the economic, social, cultural, political, and military power those people represent. This attribute of diplomatic power puts Russia at a disadvantage that it can't overcome without enhancing those elements backing diplomacy.

Cultural power is intriguing because, like sci-tech power, it has so many facets and opportunities for asymmetric conflict. In the mid-late 20th Century the United States had an overwhelming cultural presence globally, and its culture is still dominant throughout much of the world. But its history of openness and free speech also generated significant vulnerabilities. Conversely, Russia has a history of authoritarianism and strong state-security apparatuses designed to control its wide ranging empire and highly diverse population. These two traditions allowed Russia to inoculate itself from information dominance by the West, and enabled it to wage effective information warfare on the United States and its allies. Like sci-tech power, apparent dominance can be a weakness if your opponent uses your culture against you.

Russia simply can't compete with the West economically, militarily, diplomatically or culturally. Nor is Russia going to outpace the West in scientific or technological achievement. But it did out-innovate the West in its use of existing sci-tech tools for national advantage. This form of innovation is an effective, and possibly underappreciated, use of sci-tech power. Russia had major disadvantages on all fronts, but it effectively neutralized vulnerabilities exposed by ICTs and capitalized on adversary vulnerabilities through the same technologies. It played a bad hand well and utilized ICT inventions better than their Western creators. In the business sense, Russia was a late market entrant with an inferior product, but succeeded through a savvy business plan and clever marketing.

VI. Recommendations for the next twenty years

Science and technology are generating massive changes across the full spectrum of human experience, and rates of change are expected to accelerate at a geometric rate. Science and technology will only become more important as core elements of national power for the United States and other countries. Over the next 20 years, nations like China, the EU and India may rival the United States

for sci-tech supremacy. The United States will need to continue its relentless pursuit of sci-tech power because it is a primary driver of other forms of power—most notably military and economic power.

But the lesson from Russia's use of ICTs to wage information warfare on the West does not necessarily speak to the need for redoubling our emphasis on new inventions. Instead, it is a cautionary tale about how the laissez faire application of new technology can create vulnerabilities for the nations creating and deploying it. We should consider how a more rigorous examination of the impacts of new technology on society, and the vulnerabilities it creates, might have allowed us to anticipate Russia's strategy and proactively counter it.

We must pursue new technology with vigor. Advances in areas like artificial intelligence may provide us filtering and bot detection tools to counter Russian information warfare. But it's equally likely that those same AI tools will enable countries like Russia to enhance their disinformation operations with machine learning, chatbots, affective computing and psychometric personalization. We must match the energy we put into invention with equal effort for strategic foresight. If we simply invent for invention's sake, we're relying on chance and hope that our new or better capability will address our needs and won't expose vulnerabilities. Only a careful evaluation of how technology can accomplish or jeopardize our strategic goals will allow us to focus our sci-tech power on inventions that serve those goals. And only a careful assessment of how current technology impacts strategic goals will allow us to create innovative and effective new doctrines for accomplishing our national objectives using existing technology and tools.

Note: All of the opinions expressed are personal and do not necessarily represent the positions of the U.S. Department of State or the U.S. government.

Additional Reading

"Active Measures", Wikipedia, accesses March 1, 2017, https://en.wikipedia.org/wiki/Active_measures (https://en.wikipedia.org/wiki/Active_measures)

Adrian Chen, "The Agency," The New York Times Magazine, June 2, 2015, https://www.nytimes.com/2015/06/07/magazine/the-agency.html (https://www.nytimes.com/2015/06/07/magazine/the-agency.html)

Adrian Chen, “The real paranoia inducing purpose of Russian hacks,” The New Yorker, July 27, 2016, http://www.newyorker.com/news/news-desk/the-real-paranoia-inducing-purpose-of-russian-hacks (http://www.newyorker.com/news/news-desk/the-real-paranoia-inducing-purpose-of-russian-hacks)

Alina Polyakova, Marlene Laruelle, Stefan Meister, and Neil Barnett, “The Kremlin’s Trojan Horses,” The Atlantic Council, November 2016, accessed at: http://www.atlanticcouncil.org/publications/reports/kremlin-trojan-horses (http://www.atlanticcouncil.org/publications/reports/kremlin-trojan-horses)

Amanda Erickson, “If Russia Today is Moscow’s propaganda arm, it’s not very good at its job,” The Washington Post, January 12, 2017, https://www.washingtonpost.com/news/worldviews/wp/2017/01/12/if-russia-today-is-moscows-propaganda-arm-its-not-very-good-at-its-job/?utm_term=.385192bc3ea3 (https://www.washingtonpost.com/news/worldviews/wp/2017/01/12/if-russia-today-is-moscows-propaganda-arm-its-not-very-good-at-its-job/?utm_term=.385192bc3ea3)

Andrew Weisburd, Clint Watts, JM Berger, “Trolling for Trump: How Russia is trying to destroy our democracy”, War on the Rocks, November 6, 2016, https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/ (https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/)

Andrew Wilson, “Russian Active Measures, modernized tradition,” The Institute for Statecraft, January 3, 2016, http://www.statecraft.org.uk/research/russian-active-measures-modernised-tradition (http://www.statecraft.org.uk/research/russian-active-measures-modernised-tradition)

Carol Cadwalladr, “Robert Mercer: the big data billionaire waging war on mainstream media”, The Guardian, February 26, 2017, https://www.theguardian.com/politics/2017/feb/26/robert-mercer-breitbart-war-on-media-steve-bannon-donald-trump-nigel-farage (https://www.theguardian.com/politics/2017/feb/26/robert-mercer-breitbart-war-on-media-steve-bannon-donald-trump-nigel-farage)

Christopher Paul, Miriam Matthews, “The Russian “Firehose of Falsehood” Propaganda Model”, RAND, 2016, accessed at: http://www.rand.org/pubs/perspectives/PE198.html (http://www.rand.org/pubs/perspectives/PE198.html)

Chris Zappone, “Fake news: Why the West is blind to Russia’s propaganda today”, The Sydney Morning herald, January 31, 2017, http://www.smh.com.au/world/fake-news-why-the-west-is-blind-to-russias-propaganda-today-20170123-gtxbuw.html (http://www.smh.com.au/world/fake-news-why-the-west-is-blind-to-russias-propaganda-today-20170123-gtxbuw.html)

Daisy Sindelar, “The Kremlin’s Troll Army,” The Atlantic, August 12, 2014, https://www.theatlantic.com/international/archive/2014/08/the-kremlins-troll-army/375932/ (https://www.theatlantic.com/international/archive/2014/08/the-kremlins-troll-army/375932/)

The Economist, “Yes I’d lie to you”, September 10, 2017, http://www.economist.com/news/briefing/21706498-dishonesty-politics-nothing-new-manner-which-some-politicians-now-lie-and (http://www.economist.com/news/briefing/21706498-dishonesty-politics-nothing-new-manner-which-some-politicians-now-lie-and)

Evan Osnos, David Remnick, and Joshua Yaffa, “Trump, Putin and the new Cold War,” The New Yorker, March 6, 2017, http://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war (http://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war)

Hannes Grassegger, Mikael Krogerus, “The Data That Turned the World Upside Down”, Vice: Motherboard, January 28, 2017, https://motherboard.vice.com/en_us/article/how-our-likes-helped-trump-win (https://motherboard.vice.com/en_us/article/how-our-likes-helped-trump-win)

“Mitrokhin Archive”, Wikipedia, accessed March 1, 2017, https://en.wikipedia.org/wiki/Mitrokhin_Archive (https://en.wikipedia.org/wiki/Mitrokhin_Archive)

Margaret Kosal, “Science, Technology and the Future of Warfare,” The Modern War Institute, October 2, 2016, http://mwi.usma.edu/science-technology-future-warfare/ (http://mwi.usma.edu/science-technology-future-warfare/)

Michael Weiss, “Russia’s Long History of Messing With Americans Minds Before the DNC Hack”, The Daily Beast, July 26, 2016, http://www.thedailybeast.com/articles/2016/07/26/putin-s-wicked-leaks-didn-t-start-with-the-dnc.html (http://www.thedailybeast.com/articles/2016/07/26/putin-s-wicked-leaks-didn-t-start-with-the-dnc.html)

Office of the Director of National Intelligence, “Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident Attribution,” January 6, 2017, accessed at: https://assets.documentcloud.org/documents/3254237/Russia-Hack-Report.pdf (https://assets.documentcloud.org/documents/3254237/Russia-Hack-Report.pdf)

“Operation Infektion”, Wikipedia, accessed March 1, 2017, https://en.wikipedia.org/wiki/Operation_INFEKTION#Story_genesis_and_progression (https://en.wikipedia.org/wiki/Operation_INFEKTION#Story_genesis_and_progression)

Paul Gallagher, “Revealed: Putin’s army of pro-Kremlin bloggers”, The Independent, March 27, 2015, http://www.independent.co.uk/news/world/europe/revealed-putins-army-of-pro-kremlin-bloggers-10138893.html (http://www.independent.co.uk/news/world/europe/revealed-putins-army-of-pro-kremlin-bloggers-10138893.html)

Peter Pomerantsev, Michael Weiss, “The Menace of Unreality,” The Interpreter, November 22, 2014, accessed at: http://www.interpretermag.com/the-menace-of-unreality-how-the-kremlin-weaponizes-information-culture-and-money/ (http://www.interpretermag.com/the-menace-of-unreality-how-the-kremlin-weaponizes-information-culture-and-money/)

Peter Pomerantsev, “Inside the Kremlin’s hall of mirrors”, The Guardian, April 9, 2014, https://www.theguardian.com/news/2015/apr/09/kremlin-hall-of-mirrors-military-information-psychology

(https://www.theguardian.com/news/2015/apr/09/kremlin-hall-of-mirrors-military-information-psychology)

Phil Howard, “Project on Computational Propaganda”, Prezi Online Presentation, accessed March 1, 2017, https://prezi.com/j6xt37fqmlyw/project-on-computational-propaganda/ (https://prezi.com/j6xt37fqmlyw/project-on-computational-propaganda/)

Roman Dobrokhotov, “Russia’s soft warfare”, Aljazeera, February 27, 2017, http://www.aljazeera.com/indepth/opinion/2017/02/russia-soft-warfare-cyberwar-hackers-fake-news-170227070148722.html (http://www.aljazeera.com/indepth/opinion/2017/02/russia-soft-warfare-cyberwar-hackers-fake-news-170227070148722.html)

Samuel Woolley, Phil Howard, “Political Communication, Computational Propaganda, and Autonomous Agents”, International Journal of Communication, Volume 10, 2016, accessed at: http://politicalbots.org/wp-content/uploads/2016/10/WoolleyHoward.pdf (http://politicalbots.org/wp-content/uploads/2016/10/WoolleyHoward.pdf)

Medium (https://medium.com/short-bytes/how-russia-hacks-our-democracy-2c5460596bc3) · by Matt Chessen