Global Insight
Volume 2 • 2021
ISSN 2690-8204
doi:10.32855/globalinsight.2021.001

Russian Disinformation – The Technological Force Multiplier

Elizabeth Kilkenny

Part one of this article is a Literature Review assessing the state of the collected works of arguments surrounding the comparison and contrasting of older Soviet and contemporary Russian disinformation campaigns. There were two main overarching ideas that kept reemerging: either there is no practical difference or technological change is the only real difference, and even then, some believe it is just a natural evolution of these systems of disinformation. Other less frequent ideas surrounding this analysis are also highlighted as potentially important variables. After reviewing these previous works, the second part of this piece delves deeper into the topic by laying out examples of disinformation campaigns of the recent and distant pasts. The Literature Review and resulting analysis will ultimately show a correlation between the growth of technology and the speed of changes in the tactics used for Russian disinformation, as well as consistency between the goals of the Russian government today and the Soviet regime.

Keywords: Russia, disinformation, information warfare, propaganda, troll farms, security

Literature Review

Introduction

The objective of this literature review is to assess the collected works surrounding older Soviet and contemporary Russian disinformation campaigns, while looking for trends in the differences and similarities that have emerged over time. The two main ideas that have arisen are that there is no difference at a practical level because the regime's goals of spying on, influencing, or punishing other actors have not changed, and that emergent technology acts as a catalyst and enables the campaigns to be enacted to greater effect. Other, less frequent ideas surrounding this comparison between Soviet and Russian disinformation have also been included as they are potentially important variables that could be significantly impacting the development and growth of disinformation today: for example psychology, free speech, the rules of war changing, or the increase in massive amounts of data being created every day.

Practically No Difference

Some writers hold the opinion that the Russian disinformation tactics of today are the same at a practical level as the Soviet tactics of the past. According to Qiu, the "fake news" that Russia has been churning out in modern times is effectively no different than the propaganda techniques of the past. For example, take the case of the Soviet rumor that the government of the United States created AIDS in 1983. The main purpose of that campaign was to sow uncertainty around the intentions of the United States by using the fear of a new disease as inspiration. Those who believe that there are no practical differences between the campaigns over the years essentially say that the modern Russian rumor mills may employ different means, but their end goals are roughly equal. This position is often taken from a consequentialist point of view – with that mindset the ends are the important part of the equation, not the means. Qiu also emphasizes the roles of incrementalism and uncertainty involved in the success of Russian disinformation campaigns. The Russian government has had many years and lots of practice against various adversaries to get to the level of skill that has emerged in the modern, ever more interconnected world.

In parallel, Popescu (1) addresses the similarities between the Soviet invasion of Afghanistan and the more recent Russian incident in Crimea, claiming that "on a technical level, many of the actions undertaken by the Soviets back then are strikingly similar to the ones Russia employed in Crimea last year." In both cases the government used agents in ambiguous or disguised uniforms to their advantage, while spreading the lie that the agents were a local revolutionary effort. In the more recent Crimea incident, this began with disinformation spreading via staging for positive support before the invasion. The staging was done by an organization that hacked smart TVs in Crimea and directed them to a supposed "rebel" TV broadcast, to give off the impression that it was an organic takeover (Kubecka). Although decades have passed and regimes have come and gone, the same playbook that was used by the Soviet government in Afghanistan still seems to be influencing Russian tactics, with the main differences emerging as a consequence of technological advances.

Technological Change Is the Difference

The advent of new technologies has expanded the variety of tools at hand for spreading disinformation. According to Cull et al. (68), "the most dramatic shift in the information environment is the move to digital and online media." Technological change has revolutionized the availability and accessibility of new information, while also making it easier to propagate fictitious news. Paul and Matthews broach what they call the "firehose of falsehood" propaganda model that seems to have developed in Russia; the firehose model is propaganda that's rapid, high volume, multi-channel, continuous, responsive, and repetitive while undercutting perceptions of reality and contradicting itself sometimes. The key to this kind of propaganda is the modern technology that enables it; the internet and social media, and the ever-increasing power of hardware, all contribute to the changes in Russian tactics. Paul and Matthews also emphasize that this is built on Soviet Cold-War era thoughts and techniques. The intentions of the Russian government seem as if they have not changed much, while Russian government capabilities have expanded with technological advances over time. Russia has gotten good at adapting new technologies to its information manipulation goals worldwide.

In addition to this, there are some voices that argue Russia has simply continued down the same pathway that it started over a century ago, that this is the natural evolution of a system of disinformation - a gradual increase in the volume and sophistication of disinformation campaigns as technology improves at an ever more rapid rate. McClintock emphasizes the role technology has played in the evolution of Russian disinformation campaigns, but also concentrates on the stability they have shown in their goals: to spy, influence, or punish other actors. Similarly, MacFarquhar underscores that the planting of false stories is not new; rather, the Russian government has simply put more of a concentration on disinformation in its military doctrine, as it has only grown in its successes over the years.

Other Forces Impacting Contemporary Russian Disinformation

There are a handful of other thoughts on the nature of similarities and differences between contemporary Russian disinformation and that of Soviet times that emerge less frequently, such as the impacts of psychology, free speech, changes in the rules of war, or the increase in the sheer amount of data fueling the campaigns. Grimes broaches the idea that internet users themselves are partially to blame for increasing the ease of success for Russian disinformation campaigns today. He cites the statistic that "60% of us get our news primarily through social media" and also states "spreading propaganda requires only some webspace and an audience who are only too keen to like and share." This is tangentially related to the change in technology because social media is a part of the evolution of technological change that is altering the tools available for spreading disinformation; however, Grimes concentrates on the human psychological element of spreading and believing disinformational propaganda.

It is weird to think of free speech as a security risk, but it is an inherent vulnerability that enemies can also say whatever they want in an open forum with the intention of confusing and/or persuading the citizens of the target country. Free speech in the United States has always been an enabler for disinformation campaigns. Osnos et al. quote former KGB general Oleg Kalugin as saying, "Free societies are often split because people have their own views, and that's what former Soviet and current Russian intelligence tries to take advantage of." Many people still do not fact check news shared by those they trust on social media and end up in virtual echo chambers with all their social media confirming their preconceived notions. This definitely influences the disinformation campaigns run today, though it is not strong enough to make a big difference alone.

Another argument is that it is the evolving rules of war that make modern Russian disinformation efforts different from the past, while technology advances as it always has. Under Russian "New Generation Warfare" (what many in the West refer to as "hybrid warfare"), Allenby claims that "civilizational conflict"[1] is the change differentiating current Russian disinformation tactics from Soviet ones. Disinformation is a part of this idea of civilizational conflict. Allenby does concede that these tactics integrating "political action, concealed military activities at important leverage points, and sophisticated destabilization initiatives" are just more efficient and targeted versions of some of those used in the Soviet Union.

Allenby emphasizes a second shift of import as well: the increase in sheer quantity of data and information that we create now compared to what was ever possible before. This allowed the historical "Big Lie" style propaganda involving complete control of the media to shift to the more complex "manufactured real" of modern times (Allenby). The "manufactured real" manipulates the surrounding culture through all channels to distort reality for large groups in a mass-gaslighting manner, without needing complete media control. It becomes more about sowing uncertainty than upholding a massive falsehood. These ideas indicate that the paradigm surrounding Russian disinformation campaigns has inherently changed, rather than just the technology involved.

Finally, there are a few variables that Cull et al. think impact contemporary Russian disinformation campaigns, though with smaller impacts: the end of Cold War bipolarity, the existence of a "post-factual world," and a more diffuse propagandist network holding a more diverse set of goals (Cull et al.). The "post-factual world" is a reference to modern politicians (such as Putin or Trump) denying obvious facts with blatant lies, and yet still being believed by many. These factors arise less frequently in the literature surrounding the modern Russian disinformation circuit, but still have an impact on the conversation.

Conclusion

The equation defining the changes surrounding disinformation campaigns from Soviet to contemporary Russian times is complex - filled with many variables, like new technologies and ever more massive amounts of

1 Civilizational conflict: fighting between cultures instead of countries.

data, and only a few constants, such as the general goals of the disinformation campaigns. The overall goals of the campaigns stemming from Moscow have stayed relatively constant over the last century, although there has been an increase in diversified actors taking part in the planning and distribution of disinformation campaigns for personal gain rather than party influence. Some of the scholars from this review take a consequentialist view and find that the major differences between Soviet and Russian efforts are mostly within the means available and not in the end goals and intentions of the regimes, while still others believe that many Soviet tactics have simply been recycled with updated resources as technology grows in the continued evolution of hybrid and information warfare.

Fast technological development and the introduction of the internet have become major force multipliers for the velocity of disinformation distribution. Technological diversity and growth have had the largest individual impact on disinformation capabilities. Other notable variables are found in the psychological and sociological realms, such as in the shift in international relations from bipolarity to world power multi-polarity. Russia has continued to evolve tactics in line with what would be expected from Soviet times, and disinformation will only grow in power as technology grows.

Russian Disinformation: The Technological Force Multiplier

Introduction

The history surrounding the term "disinformation" can be seen by following the cases of formerly Soviet and contemporarily Russian "дезинформация."[2] This is a tactic of intentional manipulation of information for some (usually military or political) advantage. It has been around since the advent of human rivalry, though not as heavily used as an explicit approach or term until the most recent centuries. In modern times most media-based disinformation is just called "fake news" colloquially by the internet-based public.

The Russian government has a long history of manipulating traditional informational channels, such as newspapers, radio, and television. In more recent times this has expanded to include the cybersphere (the internet, private networks, social media, and other networked technologies). Disinformation affects populations psychologically through the manipulation of their worldview. If a government can influence the sentiment of the masses in others' states, those states are then increasingly controlled, and destabilization can take place with more ease. It should also be noted that the intentions and end goals to spy, influence, or punish other actors (McClintock) have remained largely unchanged, even while the means and capabilities have adapted to contemporary times. Complexity and risk grow when other hybrid warfare tactics are added to the equation (cyberwarfare, covert ops, economic pressure, etc.). In modern times, this information warfare is near borderless, difficult to attribute, and easier to enact.

Deception is a major challenge within politics, intelligence, and the media – a risk that could stem from within or without a state, from independent actors, a team, or an entire government. The continued freedom of speech and the press in places like the United States are both a liberty and a vulnerability. This freedom makes it much easier for foreign powers to infiltrate liberal states' public media, and thus influence public thoughts in places with such freedoms. For disinformation to be successful, there must be a potential for protest in the targeted populace. It is rare for a campaign to find success without some level of pre-existing turmoil in the targeted area to capitalize on – a fire cannot start without something for a spark to burn. Some illuminating cases will be brought forth to compare and contrast Soviet and Russian disinformation campaigns and their goals and techniques. This will ultimately show a correlation between the growth of technology and the speed of changes

2 (Transliterated) dezinformatsiya: disinformation.

in the tactics used for Russian disinformation, as well as consistency in the goals of the Russian government today with the Soviet regime.

Soviet Dezinformatsiya

Disinformation was at the core of Soviet era "active measures" – political warfare involving everything from forgeries and media manipulation to assassinations. Active measures were the predecessor to modern Russian hybrid warfare. One Cold War-era example of an active measure is the 1964 Operation Neptune. This was a successful Czechoslovakian intelligence attempt to discredit West Germany at the time by placing stolen documents that implicated then current West German politicians as Nazi collaborators inside an artificially aged chest in a lake to make them look like they had been hidden during World War II (Asiedu). According to Pond, the purpose of this event was to discredit West Germany and feed into anti-German sentiments, and to campaign for an extension of the period in which German Nazi war crimes could be prosecuted.

Czechoslovakian intelligence got a bit of what they wanted on all accounts, but their greatest success was the removal of a statute of limitations on Nazi war crimes. Still, they were not successful in implicating the West German government at the time as the newest iterations of Nazis (Pond). This is a good example of the level of technology the Czechoslovakian government utilized at the time (physical fabrication of the chests, and physically stolen documents), which is quite different from the modern day often internet-based Russian campaigns. Fabrication nowadays is more often of a digital means than physical. This is not to say that physical fabrication does not happen – physical forgeries are certainly still a real occurrence and risk.

Another disinformation campaign emerged in 1980 during the Cold War: forged documents claiming that the U.S. supported apartheid in South Africa and was persecuting Black Americans (Waller). As in many other instances of disinformation, this forgery was released in a non-Soviet newspaper, by someone involved in a Soviet front group. In this case it was a San Franciscan newspaper with a publisher who was a part of the World Peace Council, a well-known Soviet front (Waller). There is a certain level of consistency in the tactics used in Soviet disinformation campaigns; when the Soviets found that something worked, they stuck to it. This also creates a pattern that makes it easier to identify a trail of actions as potentially to have been Soviet, even if true attribution may never be possible. Barring intentionally misleading 'false flag' operations, one must look at who the attack would benefit to see the most likely culprits.

A popular disinformation campaign trend was established when Soviet authorities realized how sensitive the American public was to the use of biological weaponry. During the Vietnam War, they released a forged document illuminating the "existence" of American biological weapons caches; this time the false information was released to the *Free Press Journal* in Bombay (Boghardt). This trend of biological war-themed disinformation was developed further when the Soviet government decided to capitalize on the emergence of AIDS around the world.

One of the most infamous Soviet disinformation campaigns said that AIDS was a human-made disease, and specifically targeted the U.S. as the creator. The seeds for Operation INFEKTION were sown in 1983, though it did not reach peak rumor virility until 1987 (Boghardt; Grimes). According to Grimes, "The dissemination followed a well-established pattern: the story would appear in a publication from outside the USSR, and was then presented in Soviet media as the investigative work of others." This disinformation operation claimed that AIDS was created by the American secret intelligence unit – the CIA (Boghardt; MacFarquhar; Grimes). It was a Soviet effort meant to take advantage of existing biases against the U.S. and to make people more untrusting towards the U.S. government and its policies. Grimes (2017) states that even after the director of the SVR in 1992 admitted that it had been a Soviet campaign, some people still believe the lie. This is a lie that has cost lives due to the development of a mindset called "AIDS denialism" linked to mistrust of the government which has cost hundreds of thousands of preventable deaths (Grimes). This is a great example of a piece of disinformation taking on a

life of its own. It still is indirectly endangering lives through those who now believe AIDS is man-made, no matter who they think created it. This piece of "Big Lie" propaganda has a legacy that still costs lives today.

Thankfully, not every Soviet campaign was successful. According to both Niemann and Grimes, one failed campaign was an attempt to keep Ronald Reagan from being reelected President of the United States. This was done by attempting to infiltrate the headquarters for both major American political parties, trying to make the phrase "Reagan means war!" popular, and overall aiming to discredit President Reagan in the eyes of the American populace (Niemann). These attempts had little to no impact; Reagan won the election by a landslide. The American people were not fooled in this case – the positive sentiments surrounding President Reagan were too great. It was a lesson to the Soviets to be careful expending time and energy on a campaign if the cards are stacked too highly against them. This was before the internet made dissemination of these poisonous ideas so much easier – human limitations restricted the velocity of disinformation, and time wasted on a failed campaign was more costly.

As can already be seen, even before the advent of the internet the Russian government was hard at work refining many of the strategies and tactics that are still used in the modern world. Soviet disinformation campaigns are the roots of the modern operations that we see come out of Russia today. These more modern campaigns have improved iteratively in many ways, while still maintaining some consistency across goals, tactics, and targets. The shift from the Soviet regime to the modern Russian one in the 90s came at a pivotal time where the possibilities of the internet were only beginning to be explored.

Modern Cyber-Information War

Despite a bold promise to halt disinformation campaigns aimed at the United States after the breakup of the Soviet Union, Russia continued full force (Osnos et al.). In 1998, the Russian government was discovered spying on the United States government using cyber-means (McClintock). This was a typical attempt to gain sensitive information in line with past spying operations, just in the digital realm rather than the physical. This indicated the Russian government's arsenal for non-violent hybrid warfare consists of more than technical attacks – it also intertwines information and psychological war. In a society that has been becoming increasingly illiberal and undemocratic, these tactics are bound to continue. Authoritarian states have no issues lying to their own people, so of course they will lie to those they see as enemies without hesitation.

The first well known instance of a state-on-state massive cyberattack was in Estonia during the spring of 2007 (McGuinness). The Estonian government removed a World War II memorial that had been placed in Soviet times; this caused an uproar in Russia. Semi-uncoordinated hackers, mostly originating in Russia, began to attack the websites of important Estonian institutions. Coinciding with this, Russian news falsely reported that both the statue and some nearby Soviet graves were to be destroyed, to further incense the protestors. Some speculation circulated about the origins of the attack being the Russian state, but due to the nature of most cyberattacks, attribution is a problem (McGuinness). It was not a particularly sophisticated group attack. It consisted mostly of basic copy and paste "script kiddie"[3] efforts and widespread use of Distributed Denial of Service (DDoS)[4] attacks (Osnos et al.). This attack turned out to be more of a cyber riot when compared to the state-sponsored cyberattacks seen more recently, but it was a major turning point in the known ways that Russia and other governmental actors were using technological advances to their advantage in the area of information warfare.

In the next year, Russia concentrated its gaze towards the Georgians. The attack arose because of a disputed territory in South Ossetia; the Russian forces combined a physical attack with a cyber assault (Osnos et al.). This is

3 "Script kiddies" are people who can use other people's written exploits, but do not truly understand the inner workings of what they are using, nor to they write their own scripts.

4 For DDoS attacks an attacker uses a typically large group of computers (which can include nontraditional Internet of Things items like 'smart' house appliances) to overload the systems of a target.

the first recorded instance of a dual traditional and informational/cyberattack. Technology has been growing at an increased rate, and the Russians took advantage of it. Osnos et al. claim that while "Russia prevailed militarily, its narrative was overshadowed by the Georgian one from the first minutes of the campaign." They technically won militarily, but lost ideologically. They did not manage to get a good enough percentage of the world to believe their disinformation in this case. This shows how quickly Russian disinformation teams were adapting at this time, and the difference that a year made in their tactics.

The emergence of state sponsored hacker collectives happened somewhere in the mid to late 2000s, with one that is thought to be Russian in origin holding prominence still today. Maldre shares a list of some Advanced Persistent Threats (APTs) that are thought to be associated with Russia. One example of such a collective is APT28 (also known by Sofacy and a few other monikers). Cybersecurity analysts have been able pin down certain consistencies in the metadata and attributes surrounding some attacks that make them fit together in a larger picture. FireEye reported that there were regularities in the malware used, that the targeting of these groups was in line with those the Russian government might want to target (the United States, NATO, etc.), that there were Russian language markers in the malware code over a six-year period, and that the code was compiled consistently in Russian business hours. They assessed that the Russian government is the most likely backer of APT28. These findings were confirmed and expanded upon in a white paper by another security company, Bitdefender (Benchea et al.). A couple of examples of efforts attributed to APT28 are the 2015 hack of the German parliament and the 2016 hack of the U.S. Democratic National Committee (Daniels). This shows that the Russian government has maintained a concentrated effort on consistently still targeting the West, despite new tools being used.

Russia has also expended effort on further influencing the formerly Soviet countries whose intelligence teams used to be under Soviet control. These countries are particularly vulnerable to Russian disinformation due to their substantial Russian speaking populations, their physical proximity to Russia, and their historical relationship with the USSR (Radin). Countries like Estonia receive Russian propagandized media via Russian language traditional news sources and social media (Mardiste). These vulnerabilities were taken advantage of by Russia in Ukraine back in 2014 in the now infamous Crimean annexation. Initially, what is thought to be a Russian backed group hacked into smart TVs and forced them to a "rebel" TV channel, to give off the impression that it was a homegrown separatist movement (Kubecka). Then, Russia used unmarked forces (sometimes referred to as "little green men") for military actions in Crimea (Radin). By keeping the agents unmarked, Russia could pretend that it had no idea who they were. These instances have reasonably created anxiety in some of the states bordering Russia. In some cities bordering the mainland of Russia, like Daugavpils in Latvia, Russian speakers are a majority and there has been some concern that Russia will reuse the tactics from Crimea (Radin). The Baltics are a little bit more protected than Ukraine, though, due to their membership in NATO.

More recently, Russia was distinctly campaigning for a "leave" Brexit vote. Nimmo aggregated Kremlin funded media reports related to Brexit and analyzed the headlines, commentators, context, and language use for systemic bias pushing for the U.K. to go through with leaving the European Union. After breaking down reasons why this slant cannot be accidental, Nimmo determined that it was an intentional disinformation campaign to give more attention to those who were for Brexit. This is a direct tie to the desires of the Kremlin, as state funded media cannot deviate widely from the feelings of the Russian government without likely getting into trouble.

Also in 2016, the Russian plot against the American Democratic Party that was previously mentioned was one of the more successful disinformation campaigns believed to come from Russian influences. It impacted the highest elected office in the United States. According to Osnos et al. "the operation involved hacking Democrats' e-mails, publicizing the stolen contents through WikiLeaks, and manipulating social media to spread "fake news" and pro-Trump messages." Even if caught, they have not lost, as they will have shown how vulnerable the American system can be. Some of the support for this campaign came from Twitter bots and "troll farms."

Troll farms are one of the newer developments in the toolbox of contemporary Russian disinformation campaigners. These are businesses employing people to control online fake personas and botnets[5] to spread elaborate disinformation campaigns. Some have emerged connected to Russia, funded by people in close proximity to the Kremlin. These kinds of organizations were employed to spread "fake news" about Hillary Clinton in the 2016 U.S. election (Osnos et al.). Another interesting case involving the troll farms is from Louisiana: a forged accident on Twitter with pictures, a catchy hashtag, and video "evidence" when a chemical plant called Columbia Chemical supposedly had an explosive accident (Chen). This is not a basic hoax, however. The campaign was highly complex with many different involved Twitter accounts and even a fake Wikipedia page (Chen). It is likely that this campaign was an experiment for technique refinement, since there is no real long-term goal here other than causing fear, and comparable campaigns have come to pass since. According to Chen other similar campaigns emerged and were pushed by the same fake accounts. This is the level of complexity that is emerging in Russian cyber-disinformation campaigns.

Interestingly, Adrian Chen was also the target of a disinformation campaign by the group thought to be responsible for many of these campaigns – "the Agency." Chen was researching their efforts and they did not like this, of course. Also known as the "Internet Research Agency," they have since been the subject of an indictment by the U.S. government for election meddling (United States District Court for the District of Columbia). After Chen went to Saint Petersburg to interview a worker from the Agency, he was set up with pictures from their meeting and a narrative claiming that he was there to undermine the Kremlin for the CIA, NSA or some other American agency. Some of the attacks came from the same sets of Twitter accounts that were already being investigated (Chen). It can be a dangerous game trying to investigate the actions of those who churn out lies for a living.

The Russian government has adopted new technology for its ends as that technology emerges. If it is a piece of technology that can be exploited to further a disinformation campaign, it will be. Some of the strongest catalysts that have come out of modern technology are the internet in general, social media, and machine learning programming capabilities; these all culminate in the troll farms and deep fakes of today. Additionally, it does not help that audiences are often not critical of the news being shared by their trusted networks, while social media is only minimally fact checked before these things are shared.

Conclusion

One of the biggest differences between Soviet and modern Russian disinformation campaigns is that nowadays the internet and other technological breakthroughs have become force multipliers for the potential damage that a disinformation campaign can enact. As Grimes put it:

Today, spreading misinformation is orders of magnitude easier than it was in the 1980s, and in an era when 60% of us get our news primarily through social media, spreading propaganda requires only some webspace and an audience who are only too keen to like and share.

Technology is also a tool for crafting better disinformation. With programs for photo, video, and audio editing becoming ever more advanced, lies are becoming easier to "prove" with digital forgeries. Additionally, Russian agents have had time to hone basic theoretical objectives stemming from Soviet times.

You can see a distinct change in the kind of lies that have emerged over time as well. Big, basic rumors have given way for Paul and Matthews's (2016) "firehose of falsehood" system, overloading people's newsfeeds with questionable fake news. This makes it more confusing for the average person to sift through the lies and discern the real information. Russian deceptions are thought to have pulled some of the strings in such major state votes

5 Networks of (often maliciously compromised) computers controlled remotely.

as the 2016 American presidential election and the United Kingdom's Brexit vote with social media manipulation. Overall, the depth and breadth of disinformation campaigning has increased and as information technology continues to evolve, so too will disinformation tactics, techniques, and procedures.

References

Allenby, Braden R. "The Paradox of Dominance: The Age of Civilizational Conflict." *Bulletin of the Atomic Scientists*, vol. 71, no. 2, Jan. 2015, pp. 60–74. doi:10.1177/0096340215571911. Accessed 20 Apr. 2018.

Asiedu, Dita. "Details of Czechoslovakia's Biggest Disinformation Operation Published on Web." *Radio Prague International*, 8 June 2007, english.radio.cz/details-czechoslovakias-biggest-disinformation-operation-published-web-8607186. Accessed 30 Apr. 2018.

Benchea, Razvan, et al. "APT28 Under the Scope A Journey into Exfiltrating Intelligence and Government Information." *Bitdefender*, 17 Dec. 2015, labs.bitdefender.com/wp-content/uploads/downloads/apt28-under-the-scope-a-journey-into-exfiltrating-intelligence-and-government-information/. Accessed 3 July 2021.

Boghardt, Thomas. "Operation INFEKTION: Soviet Bloc Intelligence and Its AIDS Disinformation Campaign." [online] *Studies in Intelligence*, vol. 53, no. 4, Dec. 2009, pp. 1-24. digitallibrary.tsu.ge/book/2019/september/books/Soviet-Bloc-Intelligence-and-Its-AIDS.pdf. Accessed 3 July 2021.

Chen, Adrian. "The Agency." *The New York Times*, 2 June 2015. *NYTimes.com*, www.nytimes.com/2015/06/07/magazine/the-agency.html. Accessed 28 Apr. 2018.

Cull, Nicholas, et al. "Soviet Subversion, Disinformation and Propaganda: How the West Fought Against It: An Analytic History, with Lessons for the Present, Final Report." [online] *LSE Consulting*, Oct. 2017, www.lse.ac.uk/iga/assets/documents/arena/2018/Jigsaw-Soviet-Subversion-Disinformation-and-Propaganda-Final-Report.pdf. Accessed 9 May 2018.

Daniels, Laura. "Russian Active Measures in Germany and the United States: Analog Lessons from the Cold War." *War on the Rocks*, 27 Sept. 2017, warontherocks.com/2017/09/russian-active-measures-in-germany-and-the-united-states-analog-lessons-from-the-cold-war/. Accessed 1 May 2018.

FireEye. "APT28: A Window into Russia's Cyber Espionage Operations?" *FireEye*, www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html. Accessed 18 Apr. 2018.

Grimes, David. "Russian Fake News is Not New: Soviet Aids Propaganda Cost Countless Lives." *The Guardian*, 14 June 2017, www.theguardian.com/science/blog/2017/jun/14/russian-fake-news-is-not-new-soviet-aids-propaganda-cost-countless-lives. Accessed 29 Apr. 2018.

Hansen, Flemming. *Russian Hybrid Warfare: A Study of Disinformation*. Research Report, 2017:06, DIIS Report, 2017. http://hdl.handle.net/10419/197644. Accessed 3 July 2021.

Kubecka, Chris. "How to Start a Cyberwar: Lessons from Brussels EU & NATO Cyberwar Exercises." Live conference talk, *BSides Las Vegas*, 2018. youtu.be/em1GObQAIOc. Accessed 3 July 2021.

MacFarquhar, Neil. "A Powerful Russian Weapon: The Spread of False Stories." *The New York Times*, 28 Aug. 2016, www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html. Accessed 18 Apr. 2018.

Maldre, Patrik. "The Russian Cyber Threat: Views from Estonia." *The Northern European: UpNorth*, 17 June 2016, upnorth.eu/the-russian-cyber-threat-views-from-estonia/. Accessed 19 Apr. 2018.

Mardiste, David. "Estonia Braced to Resist 'Fake News'." *Reuters*, 28 Feb. 2017. www.reuters.com/article/us-estonia-pm-idUSKBN1671S2. Accessed 18 Apr. 2018.

McClintock, Bruce. "Russian Information Warfare: A Reality That Needs a Response." *RAND*, 21 July 2017, www.rand.org/blog/2017/07/russian-information-warfare-a-reality-that-needs-a.html. Accessed 19 Apr. 2018.

McGuinness, Damien. "How a Cyber Attack Transformed Estonia." *BBC News*, 27 Apr. 2017, www.bbc.com/news/39655415. Accessed 15 Apr. 2018.

Nimmo, Ben. "Lobbying for Brexit: How the Kremlin's Media are Distorting the UK's Debate." *The Institute for Statecraft*, 2016, www.statecraft.org.uk/research/

lobbying-brexit-how-kremlins-media-are-distorting-uks-debate. Accessed 10 May 2018.

Osnos, Evan, et al. "Trump, Putin, and the New Cold War: What Lay Behind Russia's Interference in the 2016 Election—and What Lies Ahead?" *The New Yorker,* www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war. Accessed 10 May 2018.

Pond, Elizabeth. "DISINFORMATION. Truth Is the Best Defense. CASE STUDY: WEST GERMANY. A Czech Ploy That Worked -- but Only Briefly." *Christian Science Monitor*, Mar. 1985, www.csmonitor.com/1985/0301/zdis4c.html. Accessed 3 May 2018.

Popescu, Nicu. "Hybrid Tactics: Neither New nor Only Russian." *European Union Institute for Security Studies*, Jan. 2015, www.files.ethz.ch/isn/187819/Alert_4_hybrid_warfare.pdf. Accessed 28 Apr. 2018.

Qiu, Linda. "Fingerprints of Russian Disinformation: From AIDS to Fake News." *The New York Times*, 12 Dec. 2017, www.nytimes.com/2017/12/12/us/politics/russian-disinformation-aids-fake-news.html. Accessed 18 Apr. 2018.

Radin, Andrew. "Hybrid Warfare in the Baltics: Threats and Potential Responses." *RAND Corporation*, 2017, www.rand.org/content/dam/rand/pubs/research_reports/RR1500/RR1577/RAND_RR1577.pdf. Accessed 18 Apr. 2018.

UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA. *Internet Research Agency Indictment*, District of Columbia, 16 Feb. 2018, www.justice.gov/file/1035477/download. Accessed 4 Aug. 2018.

Waller, Michael. *Strategic Influence: Public Diplomacy, Counterpropaganda, and Political Warfare*, Institute of World Politics Press, 2009, pp. 156–162.