Active Measures: Moscow Blends Media/Technology in Information Warfare to Influence Elections

Eric Warren

Fall 2019

CENTER FOR ANTICIPATORY INTELLIGENCE

COLLEGE OF HUMANITIES AND SOCIAL SCIENCES
UtahStateUniversity.

Active Measures: Moscow Blends Media/Technology in Information Warfare to Influence Elections

Center for Anticipatory Intelligence
Student Research Reports

Eric Warren
December 2019

Executive Summary

In its report on Russian active measures campaigns to interfere with the 2016 United States election, the US Senate Select Committee on Intelligence found that the Russian government conducted a comprehensive disinformation campaign against US election infrastructure that started in at least 2014 and carried through to 2017.[1] Ensuing reports conclude that Russian active measures, or political warfare designed to influence foreign affairs without reaching the threshold of a hot war, continue to permeate American political discourse.[2] Russia's intent is to influence the outcome of upcoming elections by leveraging, enhancing, and fabricating differences in American society. This poses a serious national security threat.[3]

While Russian influence in the 2016 US presidential campaign gained wide attention, Russia has a long history of disinformation campaigns targeting US elections, beginning in at least 1919. Over the next century, Russia honed its disinformation tactics, culminating in the manipulation of voters through the use of new media as a way to use America's "civilization, identity, and will by generating complexity, confusion, and political and social schisms."[4] Russia's contemporary disinformation efforts to affect internal political debate reaches beyond US borders and strikes within US allies' and other nations' boundaries. US NATO partners and nations throughout Africa have been the target of Russian interference through social media and Russian state-sponsored news organizations to create confusion and propagate tumult. Moreover, it appears that the Kremlin is using these states as a proving ground for continued weaponized narrative attacks on America in the run-up to the 2020 US presidential election.[5]

Russia has found manipulatable, target-rich audiences in the US and other countries where it seeks to interfere in internal politics with its use of memes and state-driven narratives.[6] Unlike disinformation tradecraft devices in the past, social media platforms enable Russia to covertly deliver its spurious messages instantly to an audience of millions, gauge reaction, and then modify tactics.[7] Furthermore, Russia's marks are growing. The number of social media users worldwide rose from 970 million in 2010 to an estimated 2.09 billion in 2021.[8]

The solution to defeating Russian active measures rests with an integrated and holistic approach that incorporates efforts from across the US national security enterprise. Among these actors, the US Intelligence Community (IC) can take a key role in providing information and analysis for policymakers to better understand the Russian entities involved with disinformation operations, their modus operandi, and their fundamental motives in order to equip the US to effectively counter the threat of Russian active measures.

Introduction: Russia's Information Battlefield Leverages Integrated Asymmetric Warfare

The Russian approach to information warfare is layered with various organizations deploying tactics for a singular objective: the pursuit of power.[9] In 2016, the St. Petersburg-based Internet Research Agency (IRA) sought to interfere with the US presidential election by amplifying preexisting rifts within American society to sow discord.[10] For Russia, information operations are a necessary extension of nearly every significant national effort, both within the federation and beyond its borders.[11] It deploys disinformation campaigns in both peacetime and during war and views the use of active measures as a good and natural extension of foreign affairs.[12] In a study on hostile social manipulation, the Rand Corporation writes that Russian doctrine has formalized the importance of information influence operations:

> In peacetime, information operations must be maintained to achieve objectives set by the country's political leaders in an effort to enhance the effectiveness of political, diplomatic, economic, judiciary, and military measures to maintain the security of the Russian Federation.[13]

In post-Soviet Russia, US political strategy has been a factor in Russian approaches to social manipulation. Since the early 1990s, American public relations experts have worked in Russia, sharing their expertise on the nuances of social manipulation.[14] In 1996, public relations and political consulting experts were surreptitiously recruited to help the successful 1996 reelection campaign of former Russian president Boris Yeltsin.[15] The influence of American public relations experts during the 1996 Yeltsin campaign, a standard campaign strategy in the US, was likely viewed by Russians as an interference of a Russian election by the US.[16]

For at least the past two decades, Russians have considered information warfare against their state as a real threat to Russian national security.[17] Russia views competing states, such as the US, as attempting to control the global information space and squeeze Russia from the international information market.[18] In response, Russia developed a concept to address the confrontation between states in the information space with the purpose of inflicting severe damage to information systems, operations and resources, and necessary infrastructure; subverting social systems and the economy; and "creat[ing] substantial psychological manipulation of the population to destabilize the state and society."[19]

In 2013, Russia's Chief of General Staff, General Valery Gerasimov, wrote a now often-referenced article in which he declared, "In the 21st century we have seen tendency toward blurring the lines between the states of war and peace. Wars are no longer declared and, having begun, proceed according to an unfamiliar template."[20] In what is popularly known now as the Gerasimov Doctrine, he went on to argue, "The very rules of war have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness."[21]

The architecture of Russian information, and disinformation, campaigns is cohesive with strategic messaging coming from the Kremlin, and dispersing to key organizations for deployment that include Roskomnadzor, state-sponsored media, troll farms, and Russia's intelligence services.[22] According to the Russian Federation, Roskomnadzor is the federal executive organization responsible for managing the media, including the electronic media, and mass

communications, information technology, and telecommunications.[23] It has created the most far-reaching and powerful social media monitoring system in the world.[24] Thus, Russia has a capable defense against the very type of influence campaigns it uses against other nations.

Large, state-sponsored media outlets such as Sputnik News and RT (formally known as Russia Today) have long histories of articulating narratives from the Kremlin. In a 2014 diplomatic post on the US State Department's Dipnote blog site, former Under Secretary of State for Public Diplomacy and Public Affairs and managing editor of Time magazine Richard Stengel accused RT of lodging a disinformation campaign by airing propaganda posing as news.[25] Furthermore, the US Intelligence Community reported with high confidence that RT and Sputnik contributed to the influence campaign of the 2016 US elections by "serving as a platform for Kremlin messaging to Russian and international audiences."[26]

Russian entities such as the state-sponsored Internet Research Agency employed a sophisticated campaign using social media platforms to sow dissonance and disconnection with reality in American political dialogue to create instability.[27] In an indictment against the IRA and its agents, the US Department of Justice alleges that the IRA had a strategic goal to propagate friction in the US political system, including the 2016 US presidential election; posted derogatory information about some candidates on social media; purchased political advertisements on social media in the names of US citizens and entities; and staged political rallies inside the US while posing as US grassroots entities and citizens.[28]

Three of Russia's intelligence services have roles in deploying active measure disinformation campaigns. Russia's Main Intelligence Directorate, commonly known as the GRU, and the Foreign Intelligence Service, or SVR, have primary roles in disinformation, while Russia's Federal Security Service—the FSB—has a subsidiary role in the use of active measures.[29] Two organizations working together within the GRU, Military Unit 74455, and Military Unit 26165—together known as Fancy Bear, have used social media accounts and other mechanisms to release information stolen by various hacking activities as part of the influence campaign during the 2016 US presidential election, and in other areas.[30, 31] Another Russian intelligence group, known as Cozy Bear, who hacked the Democratic National Committee in 2016, is thought by Dutch intelligence officials to be part of the SVR.[32] Recent reports suggest that Cozy Bear is currently active and targeting the US and some of its allied countries.[33]

Only Delivery Methods Have Changed in Russia's Long-Running Election Influence Campaigns

Although the 2016 US election has brought to the forefront foreign interference in elections, it is important to reiterate that Russia has a protracted history of meddling in political processes of countries it views as adversarial.[34] In 1919, Moscow founded Communist International (Comintern) and urged members of the American Communist Party to pursue revolutionary regime change in the United States.[35, 36] They were, ultimately, unsuccessful.

During the 1960 Presidential elections, Soviet leader Nikita Khrushchev preferred Democratic nominee John F. Kennedy over Republican nominee Richard Nixon.[37] In what has been called The Kitchen Debate, Khrushchev and Nixon attended the 1959 opening of the American exhibition at Sokolniki Park in Moscow. While standing inside a model American kitchen, the two leaders publicly argued the merits of capitalism versus communism. During the

heated debate, Khrushchev told Nixon, "You do not know anything about communism—except fear of it."[38] He later said that if Nixon became President, he did not believe Nixon would contribute to an improvement of US-USSR relations.[39] Another telling example of Khrushchev's preference of Kennedy over Nixon occurred during negotiations between the US and USSR on the exchange of prisoners. The Soviet Union had imprisoned two US Air Force officers for espionage, but in order to avoid allowing Nixon (who was the incumbent US Vice-President) to take credit and highlight his ability to work with the Soviets, the Kremlin held on to the pilots until several days after Kennedy's inauguration. Khrushchev later said Kennedy acknowledged the Soviet help: "You are right. I admit you played a role in the election and cast your vote for me." In his memoir, Khrushchev admitted that Russians had "cast a vote" for Kennedy and said,

> As it turned out, we'd done the right thing. Kennedy won the election by a majority of only 200,000 or so votes, a negligible margin if you consider the huge population of the United States. The slightest nudge either way would have been decisive.[40]

US President Ronald Reagan was the target of Soviet disinformation campaigns from at least 1976.[41] During the Republican primaries leading up to the Presidential election of 1976, secret Soviet unit Service A, the active measures branch of the First Chief Directorate of the KGB (the USSR's primary intelligence agency), was ordered to investigate compromising material, including reports that Reagan had health issues as a result of his father's alcoholism.[42] Service A found evidence of Reagan's alleged "weak intellectual capabilities," and successfully planted anti-Reagan stories with Danish, French, and Indian news outlets.[43] In 1984, the USSR saw as its primary objective to stall American advances throughout the world and declared that the KGB must work to "expose" American vulnerabilities.[44] Exposure was a colloquial term the KGB used that meant the use of disinformation fabricated by Service A.[45]

During the 1984 presidential contest between Reagan and Walter Mondale, the KGB ordered its officers to infiltrate the campaigns of both candidates.[46] Moreover, during Reagan's 1984 campaign, the KGB announced five areas of Reagan's foreign policy on which it would focus its disinformation: Reagan's perceived militarist adventurism; his perceived responsibility for advancing the pace of the arms race, his supposed support of repressive governments around the globe, his disdain for national liberalism movements, and his lack of support for NATO.[47] During the 1984 elections, Service A was responsible for the popularity of the anti-Reagan slogan, "Reagan Means War," attempting to discredit Reagan as a warmonger.[48]

In the 21st century, the well-documented interference by the Russian Federation in the 2016 US presidential election highlights the employment of new technologies and media in its long-running use of disinformation for active measures.[49] As noted previously, as early as 2014 Russia's state-sponsored troll farm, the IRA, began operations to use social media to influence the 2016 elections.[50] The IRA created numerous social media accounts and purchased advertisements to effect its goal of creating discord among the US electorate. It posted on three popular social media platforms; Twitter, Facebook, and Instagram.[51] Amid a federal investigation into the IRA, it appears that Russia was brazenly mocking the US electoral system.[52] In 2016, Russian agents who posed as social media administrators and social justice activists recruited US citizens to hold signs in front of the White House that read "Happy 55th Birthday Dear Boss," in reference to IRA founder and owner Yevgeny Prigozhin.[53]

Weaponizing Narrative Beyond the US: Russian Election Interference in Europe and Africa

The use of new media by Russia to subvert democracy goes beyond the borders of the US.[54] In the months leading up to the 2019 elections for the European Parliament, numerous websites and social media accounts tied to Russia were spreading deceptive information intending to deepen distrust in the mainstream parties that have governed for decades.[55] The European Commission High Representative of the Union for Foreign Affairs and Security Policy reports that Russian disinformation agents have been active in a campaign using Facebook, Twitter, and YouTube to erode the credibility of the European Union. [56] The report delineated steps that must be taken to address disinformation ahead of its elections by improving the capabilities of institutions to detect, analyze, and expose disinformation, strengthen coordinated and joint responses to disinformation, and several other measures.[57]

Kremlin-backed social media trolls sought to utilize a similar strategy that they employed during the 2016 US Presidential election in the lead-up to the 2017 French presidential election.[58] Russian agents orchestrated a disinformation campaign against French presidential candidate Emmanuel Macron,[59] and Macron accused Russian news outlets RT and Sputnik of being "organs of influence and propaganda, of lying propaganda," against him during the 2017 presidential election.[60] Russia also deployed disinformation operations in Germany before its 2017 elections. In the most infamous case, Russian state television ran stories about the rape of a thirteen-year-old German girl by three Muslim men in Berlin.[61] The story was later debunked, but not before it was widely promulgated on YouTube and other media platforms, causing outrage across German society.

The Russian government has sought to infiltrate the rise of populist sentiments and economic frustrations in the UK, manipulating the UK's democratic institutions of free speech by introducing fake or misleading news.[62] During the 2016 debates on Brexit, Moscow's English-language television stations RT and Sputnik produced overwhelmingly one-sided coverage of the pro-Brexit campaign and sought to marginalize the "Remain" campaign.[63] More recently, a Russia-style disinformation campaign deployed in the UK during the general election in December 2019 has been extensively reported.[64]

Ahead of the 2020 US presidential election, Russia is accused of testing new disinformation tactics in Africa.[65] In October 2019, Facebook announced that it had removed three networks of accounts from its platform and Instagram that originated in Russia and targeted Madagascar, the Central African Republic, Mozambique, the Democratic Republic of the Congo, Côte d'Ivoire, Cameroon, Sudan, and Libya.[66] Stanford University's Internet Observatory said the tactics in Africa were launched by the IRA's Prigozhin.[67] The Internet Observatory also claimed that it has identified the Facebook operation as being tied to the Wagner Group, a Russian private military contractor that has waged secret wars on behalf of the Kremlin in Syria, the Central African Republic, and other areas.[68, 69] Likely not coincidently, the Wagner Group is owned by Prigozhin.[70]

Tools of the Craft: The Weaponization of Social Media in the 21st Century

Memes, the common internet-traded media currency in today's social, cultural, and political discourse, have become ubiquitous on social media platforms to convey feelings in interpersonal settings and to publicly protest against various governmental actions.[71] Evolutionary biologist Richard Dawkins coined the term meme in his 1976 book *The Selfish Gene* to describe cultural units of information that could transfer from one person to another.[72] Recognizing the possibility of meme weaponization, US Marine Corps Major Michael Prosser proposed a Meme Warfare Center that included two elements: an Internal Meme Center to "advise the Joint Force Commander on the composition and posture of friendly forces, to include coalition and interagency partners," and an External Meme Center to advise commanders on enemy combat forces, noncombatant indigenous personnel, and the strategic audience.[73] Although memes were still in their infancy when Prosser authored his thesis, the elements of those early internet memes were coalescing to form the popular memes of today.

Social media platforms are the delivery system of deceptive and acerbic memes meant to accomplish subversive political goals. The weaponization of social media, including memes, is intended to plant doubt and create confusion about a wide range of social and political topics. It is a potent tool to realize Gerasimov's vision in asymmetric warfare—the application of informational measures, applied in coordination with the protest potential of the population.[74] This theme has developed into consistently dynamic and powerful applications of social media. The capacity to cloud objectivity and facilitate the exploitation of preexisting biases within societies via social media has become a signature of Russian *dezinformatsiya*.[75]

In October 2019, Facebook said it had culled 56 Facebook accounts, 73 pages, 11 groups, and 5 Instagram accounts from the Russian disinformation campaign in Africa discussed above that had a combined following of 1.2 million people and advertising expenditures of about USD $87,000.[76] The posts were intended to discredit political positions or candidates, while others criticized French and American policies [see Appendix Figures 1 and 2].[77]

In a November 2017 hearing of the US House of Representatives Permanent Select Committee on Intelligence (HPSCI) regarding Russian interference in the 2016 election, some advertisements on Facebook originating from the IRA were exhibited and a representative sampling of activity from the IRA made available [see Appendix Figure 3]. During the HPSCI investigation and subsequent hearing, members of the committee noted the extent of activity by the IRA, and the scope of influence they achieved through Facebook.[78] The investigation report disclosed:

- 3,393 advertisements purchased;
- More than 11.4 million American users exposed to those advertisements;
- 470 IRA-created Facebook pages;
- 80,000 pieces of organic content created by those pages; and
- Exposure of organic content to more than 126 million Americans.[79]

During the committee's inquiry, approximately 3,000 IRA-produced Twitter accounts were presented where humans were coordinating 131,000 tweets.[80] These accounts were carefully created to mimic US news organizations, political parties, and social justice groups.[81] Furthermore, the committee identified 1.3 million tweets by Russian bots that were viewed 288 million times.[82] During the hearing, committee members also revealed a selection of sponsored content from Russian news outlet RT.[83] In 2017, the IC assessed that RT is one of Russia's primary state-run propaganda machines.[84]

The use of new technologies to disarm debate in the political domain poses an increased opportunity for disinformation agents. [85] Of particular concern is the application of "deepfakes" to discredit opponents, or otherwise deceive citizens through these AI-enabled fake videos.[86] While there currently is no evidence of the use of deepfakes to influence past elections within the US, there is a concern that they will be deployed for the 2020 presidential election.[87] The technology has already been used in attempts to influence political discourse in some states. On December 31, 2018, the president of the small African country Gabon, Ali Bongo Ondimba, appeared in a deepfake video addressing his citizens via social media.[88] Before the video, the last public appearance by Bongo was in October 2018. There had been widespread speculation that Bongo was deceased or incapacitated following a stroke.[89] While the fake video was meant to dispel rumors of Bongo's incapacitation, it served to fuel rumors that ultimately led to a failed military coup.[90] In June 2019, Malaysian Minister of Economic Affairs Mohamed Azmin bin Ali was implicated in a sex scandal involving political aide Muhammad Haziq Abdul Aziz following the release of a video reportedly showing the two men in an intimate act.[91] It was concluded that the video was a deepfake created by Azmin's political rivals.[92]

The Next Battlespace: Engaging Russian Interference in the 2020 US Presidential Election

An NBC News analysis of the Russian propaganda news website RT suggested that in 2019 it was promoting the presidential aspirations of Democratic congresswoman Tulsi Gabbard.[93] In a more comprehensive study, the Foreign Policy Research Institute analyzed 1,711 RT and Sputnik News articles from January 1 to November 10, 2019, and found that Gabbard is the overwhelming favorite of Kremlin news outlets.[94] Of the news articles analyzed by the Foreign Policy Research Institute aired by RT and Sputnik News, 45 percent of Gabbard's coverage were categorized as favorable, and 10 percent unfavorable.[95] In contrast, presidential candidates Joe Biden, Bernie Sanders, and Elizabeth Warren received favorable mentions significantly fewer times—three percent for Biden, 11 percent for Warren, and 19 percent for Sanders.[96]

Russia's early entrance to influence the 2020 election with active measures to create dissonance within the civic processes may have had an impact in the early stages of the race. In a podcast interview, former presidential candidate Hillary Clinton inferred that Gabbard was a Russian asset, an accusation Clinton also leveled on former presidential candidate Jill Stein.[97] Both Gabbard and Stein replied to Clinton's allegations, exacerbating the discord within the Democratic Party. Gabbard called Clinton a warmonger who embodied corruption, and who personified "the rot that has sickened the Democratic Party for so long."[98] Stein denied being a Russian spy, calling Clinton's assertion an "unhinged conspiracy theory."[99]

Social media platforms are attempting to keep ahead of foreign disinformation campaigns in the 2020 election. Facebook announced in November 2019 that it had already removed 50 Instagram accounts and one account on Facebook that had about 246,000 followers and that originated in Russia.[100] A sample of memes from fictitious accounts reveals that the Russian disinformation campaigns in the 2020 election cycle follow a similar pattern to the 2016 campaign. Notably, they use existing bias, such as race relations, within the US electorate to provoke resentment and acrimony [see Appendix Figure 4].[101]

Twitter chief executive officer Jack Dorsey announced in October 2019 that the social media giant would ban political ads starting on November 22, 2019, in an attempt to address foreign disinformation in political discourse.[102] It is questionable, however, if the ad ban will be useful in curbing disinformation. The IRA, or an affiliated organization, has already laid down the groundwork for their 2020 influence operations by introducing trojan horse accounts.[103] The idea is to lure followers by posting uplifting content, then methodically injecting controversial political content in their feeds. For example, @IamTyraJackson began posting tweets about a famous National Football League athlete who provided philanthropy in his community by building houses for single mothers. After acquiring many followers, @IamTyraJackson interspersed harmless content with controversial political tweets.[104]

Integrated National Security Community Plan Essential to Combat Russian Interference

The legacy of Russian interference in the US and foreign politics through the use of active measures is lengthy and can be injurious to the pillars of democracy. With the growth of social media and technology in the twenty-first century, the rewards for Russia to disrupt the social fabric of America are great, as are the risks for democracy. Free and fair elections—a core tenet of democracy—must be protected from those who seek to sabotage them through malicious interference. A forensic understanding of how and why Russian-produced memes and narratives infiltrate American news feeds to undermine democracy is an important step for Americans to discern what is real, and what is the true source of the information. Despite indictments from the US Department of Justice and other public disclosures released by European governments, Russia has continued to sustain information operations targeting government, defense, and military sectors in Europe and Eurasia, as well as organizations affiliated with NATO.[105] A consolidated national strategy used by the US security enterprise, policymakers, academia, and industry to counter active measure campaigns is imperative.

The problem set has been identified. A key element to securing our democracy in the face of an aggressive, and arguably successful, disinformation campaign is to understand better the organizations, methods, motivations, and people who are engaging in the "like war" against America. This will require the collection, analysis, and evaluation of intelligence to provide decisionmakers with the best information available to make sound policy. The key players within the US Intelligence Community and broader national security framework are positioned to take the lead on these fronts.

The Central Intelligence Agency should focus resources on the gathering of human intelligence to better understand the motivations and tactics of internet trolls within organizations such as the IRA. Methods would include the deployment of CIA's Directorate of

Operations to recruit and manage assets, and focusing the Directorate of Science and Technology (DS&T) and the Directorate of Digital Innovation (DDI) toward monitoring the deployment of active measures in cyberspace. The Directorate of Analysis (DA) will take charge in the assessment of intelligence collected from those assets. To better understand the threatscape, the National Security Agency (NSA) should leverage its expertise in signals intelligence to delineate who the key Russian actors are, where they are located, and what tools and systems are being used to disseminate information. Additionally, the NSA should identify overseas cyber espionage operations against US organizations that hold information that can be used to effectuate disinformation campaigns—as was the case in the 2016 theft of emails from the Democratic National Committee by Cozy Bear, and subsequent publishing of those emails by Fancy Bear.[106] The NSA should also look for technical vulnerabilities of our adversaries that would aid in preventing disinformation attacks before they are deployed, and develop recourses to identify and mitigate deepfakes and other emerging technologies used to propagate disinformation.

Counterintelligence against foreign agents within the US homeland is key to dissuading would-be disinformation brokers from intefereing with US elections. Russian agents Aleksandra Krylova and Anna Bogacheva, working for the IRA, traveled to the US in June 2014 to collect intelligence. Had the US State Department obtained information about their employment and their employer before receiving visas, they would have been flagged from entering the US. As it was, Krylova and Bogacheva were able to meticulously plan their intelligence collection itinerary, purchase collection equipment, and discuss security measures without much fear of being caught.[107] Maria Butina, who pleaded guilty to being a Russian spy, was a prolific social media influencer who used the cover of a university student while working as a foreign agent.[108] The Federal Bureau of Investigation (FBI) should allocate more counterintelligence resources specific to the identification and capture of Russian agents-of-influence who fit the profile for a new generation, and a new type, of spy.

The US should send an unmistakable message to Russia and other cyberespionage disinformation operatives that the US intelligence apparatus know who they are and will use offensive measures to protect democracy. US Cyber Command (CYBERCOM) should seek and propose areas of offense where it can replicate the success of its operations against the IRA during the 2018 US midterm elections. During that operation, CYBERCOM effectively took the IRA offline,[109] employing direct messaging, texts, emails, and pop-ups to get the attention of the would-be saboteurs.[110]

While the measures outlined above will serve to elevate the defense of America's and our allies' electoral systems, these technical precautions, intelligence activities, and offensive measures will not insulate Americans from cyber disinformation campaigns. A whole-of-society approach—the worthy subject of further research and policy design—is needed to defeat active measures in the age of social media effectively. Public awareness of and defensive-mindedness against these campaigns, transparency in US efforts to combat foreign information operations, and a significant effort to strengthening cooperation between the US government, industry, the academy, and allied nations will be essential to defend against the use of active measures.[111]

Appendix

Figure 1. Sample content of removed material. Page title: "Libya Gaddafi" Post translation: "Why was late Libyan leader Muammar al-Gaddafi killed? Everyone was happy in Libya. There are people in America who sleep under bridges. There was never any discrimination in Libya, and there were not problems. The work was good and the money, too."[112]

Figure 2. Page title: "Falcons of the Conqueror" Post translation: "Field Marshal Haftar: Libyans decide who to elect as the next president, and it is Saif al-Islam al-Gaddafi's right to be a candidate." [113]

Figure 3. A sample paid advertisement on Facebook during the US 2016 from Russia's IRA. United Muslims of America is a fictitious organization, and no such event was planned at The White House.

Figure 4. A fictitious Facebook account affiliated with Russia's IRA seeks to deepen fissures in US race relations ahead of the 2020 elections.

Endnotes

[1] US Senate Select Comm. on Intelligence, Russian Active Measures Campaigns and Interference in the 2016 Election, Volume 2: Russia's use of Social Media with Additional Views, Rep. No. 116-XX, (2019).
[2] Linvill, Darren L., Brandon C. Boatwright, Will J. Grant, and Patrick L. Warren. "'THE RUSSIANS ARE HACKING MY BRAIN!' Investigating Russia's Internet Research Agency Twitter Tactics during the 2016 United States Presidential Campaign." *Computers in Human Behavior* 99 (October 1, 2019): 292–300. doi:10.1016/j.chb.2019.05.027.
[3] Andrew, Christopher. The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB. New York: Basic Books, 2000. Accessed December 4, 2019. ProQuest Ebook Central. p. 225.
[4] Allenby, Brad, and Joel Garreau. "Weaponized Narrative Is the New Battlespace." Defense One, January 3, 2017. https://www.defenseone.com/ideas/2017/01/weaponized-narrative-new-battlespace/134284/.
[5] Alba, Davey, and Sheera Frenkel. "For Russia, Africa Is Lab To Test Disinformation." *New York Times*, October 31, 2019, B1(L). *Gale Academic Onefile* (accessed December 9, 2019). https://link-gale-com.dist.lib.usu.edu/apps/doc/A604285358/AONE?u=utah_gvrl&sid=AONE&xid=572619ce.
[5] "Removing More Coordinated Inauthentic Behavior From Russia." About Facebook, November 13, 2019. https://about.fb.com/news/2019/10/removing-more-coordinated-inauthentic-behavior-from-russia/.
[6] Bennett, W. Lance, and Alexandra Segerberg. "The Logic of Connective Action." *Information, Communication & Society* 15, no. 5 (April 10, 2012): 739–68. https://doi.org/10.1017/cbo9781139198752.002.
[7] Cooper, Paige. "Social Media Advertising Stats that Matter to Marketers in 2018." *Hootsuite* (blog), June 5, 2018. https://blog.hootsuite.com/social-media-advertising-stats/.
[8] Clement, J. "Number of Social Media Users Worldwide 2010-2021." Statista, August 14, 2019. https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.
[9] Watts, Clint. "Russia's Active Measures Architecture: Task and Purpose." Alliance For Securing Democracy, June 11, 2018. https://securingdemocracy.gmfus.org/russias-active-measures-architecture-task-and-purpose/.
[10] "Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements." U.S. House of Representatives Permanent Select Committee on Intelligence. Accessed December 3, 2019. https://intelligence.house.gov/social-media-content/.
[11]Mazarr, Michael J., Abigail Casey, Alyssa Demus, Scott Harold, Luke J Matthews, Nathan Beauchamp-Mustafaga, and James Sladden. *Hostile Social Manipulation: Present Realities and Emerging Trends*. Santa Monica, CA: Rand Corporation, 2019. p. 56.
[12] Ibid.
[13] Kh .I. Sayfetdinov, "Information Operations on the Battlefield," Military Thought, Vol. 23, no. 3, 2014, p. 74.
[14] Mazarr, 2014. p. 46.
[15] Mazarr, 2014. p. 47.
[16] Ibid.
[17] Mazarr, 2014. p. 50.
[18] "National Security Concept of the Russian Federation." Global Beat. Accessed December 2, 2019. https://fas.org/nuke/guide/russia/doctrine/gazeta012400.htm.
[19] Ministry of Defense of the Russian Federation, "Russian Federation Armed Forces' Information Space Activities Concept, 2011," January 2012.
[20] Gerasimov, Valery. "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," trans. Robert Coalson, Military-Industrial Kurirer, 27 February 2013, accessed 2 December 2019.
[21] Ibid.
[22] Watts, 2018.
[23] "Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (ROSKOMNADZOR)." Роскомнадзор. Accessed December 3, 2019. http://rkn.gov.ru/eng/.
[24] Watts, 2018.
[25] LoGiurato, Brett. "Russia's Propaganda Channel Just Got A Journalism Lesson From The US State Department." Business Insider. Business Insider, April 29, 2014. https://www.businessinsider.com/state-department-responds-rt-russia-today-john-kerry-2014-4#!HDahV.

[26] Office of the Director of National Intelligence, “Assessing Russian Activities and Intentions in Recent US Elections”, IC Assessment (ICA) 2017-01D, 6 January 2017. p. 3. https://www.dni.gov/files/documents/ICA_2017_01.pdf
[27] Linvill, 2019.
[28] United States of America v. Internet Research Agency LLC A/K/A Mediasintez LLC A/K/A Glavset LLC A/K/A Mixinfo LLC A/K/A Azimut LLC A/K/A Novinfo LLC, Concord Management and Consulting LLC, Concord Catering, Yevgeniy Viktorovich Prigozhin, Mikhail Ivanovich Bystrov, Mikhail Leonidovich Burchik A/K/A Mikhail Abromov, Aleksandra Yuryevna Krylova, Anna Vladislavovna Bogacheva, Sergey Pavlovich Polozov, Maria Anatolyevna Bovda A/K/A Maria Anatolyevna Belyaeva, Robert Sergeyevich Bovda, Dzheykhun Nasimi Ogly Aslanov A/K/A Jayhoon Aslanov A/K/A Jay Aslanov, Vadim Vladimirovich Podkopaev, Gleb Igorevich Vasilchenko, Irina Viktorovna Kaverzina, and Vladimir Venkov. 1:18-cr-00032-DLF (US District Court, District of Columbia, 2 February 2018).
[29] Galeotti, Mark. “Putin's Hydra: Inside Russia's Intelligence Services.” ECFR.EU. European Council of Foreign Relations, May 11, 2016. https://www.ecfr.eu/publications/summary/putins_hydra_inside_russias_intelligence_services.
[30] “U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations.” The United States Department of Justice, October 4, 2018. https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.
[31] Mueller, Robert. “Report on the Investigation into Russian Interference in the 2016 Presidential Election .” govinfo. US Department of Justice, April 18, 2019. https://www.govinfo.gov/app/details/GPO-SCREPORT-MUELLER.
[32] Modderkolk, Huib. “Dutch Agencies Provide Crucial Intel about Russia's Interference in US-Elections.” de Volkskrant. De Volkskrant, January 25, 2018. https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/?referer=https://www.cyberscoop.com/cozy-bear-return-espionage-russian-hacking/.
[33] Ikeda, Scott. “Cozy Bear Is Back in the Spotlight; Notorious Russian Hackers Caught Spying on EU and Eastern European Nations.” CPO Magazine, October 23, 2019. https://www.cpomagazine.com/cyber-security/cozy-bear-is-back-in-the-spotlight-notorious-russian-hackers-caught-spying-on-eu-and-eastern-european-nations/.
[34] Cohen, Stephen F. “The Long History of US-Russian 'Meddling'.” The Nation, March 6, 2019. https://www.thenation.com/article/the-long-history-of-us-russian-meddling/.
[35] Palmer, A. Mitchell. "THE CASE AGAINST THE "REDS"." *Forum (1886-1930),* 02, 1920, 173, https://login.dist.lib.usu.edu/login?url=https://search-proquest-com.dist.lib.usu.edu/docview/90846450?accountid=14761.
[36] Andrew, Christopher M., and Vasili Mitrokhin. *The World Was Going Our Way: the KGB and the Battle for the Third World*. New York: Basic Books, 2006.
[37] Taylor, Adam. "This Kremlin leader bragged about tipping a U.S. presidential election." *Washington Post*, January 6, 2017. *Gale Academic Onefile* (accessed December 4, 2019). https://link-gale-com.dist.lib.usu.edu/apps/doc/A476677459/AONE?u=utah_gvrl&sid=AONE&xid=9c0315cc.
[38] Vivian, Anthony. "Nixon and Khrushchev: The Kitchen Debate." *Defining Documents in American History: The Cold War (1945-1991)*. Hackensack: Salem, 2016. Accessed December 04, 2019. https://online.salempress.com.
[39] Taylor, 2019.
[40] Chruev, N. S., Edward Crankshaw, and Strobe Talbott. *Khrushchev Remembers*. Boston: Little, Brown and Co., 1970. p. 234.
[41] Andrew, 2000. p. 242.
[42] Ibid.
[43] Ibid.
[44] “Russia Has Often Tried to Influence Elections, with Little Success.” The Economist. The Economist Newspaper, December 17, 2016. https://www.economist.com/united-states/2016/12/17/russia-has-often-tried-to-influence-elections-with-little-success.
[45] Ibid.
[46] Jones, Seth G. “Russian Meddling in the United States: The Historical Context of the Mueller Report.” Russian Meddling in the United States: The Historical Context of the Mueller Report | Center for Strategic and International Studies, March 27, 2019. https://www.csis.org/analysis/russian-meddling-united-states-historical-context-mueller-report.

[47] Andrew, 2000. P. 243.
[48] Gioe, David V. “Cyber Operations and Useful Fools: the Approach of Russian Hybrid Intelligence.” *Intelligence and National Security* 33, no. 7 (2019): 955. https://doi.org/10.1080/02684527.2018.1479345.
[49] Mueller, 2019.
[50] Chen, Adrian. "The Agency." *The New York Times Magazine*, June 7, 2015, 57(L). *Gale Academic Onefile* (accessed December 5, 2019). https://link-gale-com.dist.lib.usu.edu/apps/doc/A416850735/AONE?u=utah_gvrl&sid=AONE&xid=4573a7d5
[51] Lukito, Josephine. “Coordinating a Multi-Platform Disinformation Campaign: Internet Research Agency Activity on Three U.S. Social Media Platforms, 2015 to 2017.” *Political Communication*, October 14, 2019, 1–18. https://doi.org/10.1080/10584609.2019.1661889.
[52] Constine, Josh. “Facebook Reveals Russian Troll Content, Shuts down 135 IRA Accounts.” TechCrunch. TechCrunch, April 3, 2018. https://techcrunch.com/2018/04/03/facebook-russia/.
[53] Mueller, 2019. p. 19.
[54] “REPORT on EU Strategic Communication to Counteract Propaganda against It by Third Parties.” europarl.europa.eu. Accessed December 5, 2019. http://www.europarl.europa.eu/doceo/document/A-8-2016-0290_EN.html#title1.
[55] Apuzzo, Matt, and Adam Satariano. "Hackers Sow Discord as Vote Looms in Europe." *New York Times*, May 12, 2019, A1(L). *Gale Academic Onefile* (accessed December 6, 2019). https://link-gale-com.dist.lib.usu.edu/apps/doc/A585131266/AONE?u=utah_gvrl&sid=AONE&xid=7a32e4e9.
[56] Satariano, Adam. "Report Points Finger at Russia Over E.U. Vote Disinformation." *New York Times*, June 15, 2019, A1(L). *Gale Academic Onefile* (accessed December 6, 2019). https://link-gale-com.dist.lib.usu.edu/apps/doc/A589090639/AONE?u=utah_gvrl&sid=AONE&xid=b1c0d0ae.
[57] “Joint Communication to the European Parliament, the European Council, The Council, The European Economic and Social Committee and the Committee of the Regions: Action Plan against Disinformation.” European Commission High Representative of the union for Foreign Affairs and Security Policy, December 12, 2018. Brussels. https://eeas.europa.eu/sites/eeas/files/action_plan_against_disinformation.pdf.
[58] Isaac, Mike, and Daisuke Wakabayashi. “Russian Influence Reached 126 Million Through Facebook Alone.” The New York Times. The New York Times, October 30, 2017. https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html.
[59] Menn, Joseph. “Exclusive: Russia Used Facebook to Try to Spy on Macron Campaign - Sources.” Reuters. Thomson Reuters, July 27, 2017. https://www.reuters.com/article/us-cyber-france-facebook-spies-exclusive/exclusive-russia-used-facebook-to-try-to-spy-on-macron-campaign-sources-idUSKBN1AC0EI.
[60] Samuel, Henry. “Macron Slams Russian Media 'Lies' during Muscular Exchange with Putin at Versailles.” The Telegraph. Telegraph Media Group, May 29, 2017. https://www.telegraph.co.uk/news/2017/05/29/macron-putin-share-perfunctory-handshake-embarking-diplomatic/.
[61] Rethmann, Petra. “How Russians Have Helped Fuel the Rise of Germany's Far Right.” The Conversation, October 11, 2019. http://theconversation.com/how-russians-have-helped-fuel-the-rise-of-germanys-far-right-105551.
[62] Minority Staff Report. 2018. *Putin's Asymmetric Assault on Democracy in Russia and Europe: Impoleciation for U.S. National Security.* Committee on Foreign Relations, United States Senate, Washington, DC: U.S. Governmetn Publishing Office, 200. Accessed November 20, 2019. https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf
[63] Nimmo, Ben. 2016. *Putin's Media Are Pushing Britain For The Brexit.* February 12. Accessed December 6, 2019. http://www.interpretermag.com/putins-media-are-pushing-britain-for-the-brexit/.
[64] Sebenius, Alyza. “Russia-Style Disinformation Tactics Used in Run-up to U.K. Vote.” SFChronicle.com. Washington Post, December 3, 2019. https://www.sfchronicle.com/business/article/Russia-style-disinformation-tactics-used-in-14877198.php.
[65] Alba, 2019.
[66] “Removing More Coordinated Inauthentic Behavior From Russia.” About Facebook, November 13, 2019. https://about.fb.com/news/2019/10/removing-more-coordinated-inauthentic-behavior-from-russia/.
[67] “Evidence of Russia-Linked Influence Operations in Africa.” FSI, October 30, 2019. https://cyber.fsi.stanford.edu/io/news/prigozhin-africa.
[68] Ibid.
[69] "Putin's private army is in a war with no rules; The mercenaries of the shadowy Wagner Group, which has been linked to the president's personal chef, are exporting the Kremlin's brand of brutality and conquest across the

globe, says Roger Boyes weekend essay." *Times* [London, England], November 16, 2019, 30. *Gale Academic Onefile* (accessed December 9, 2019). https://link-gale-com.dist.lib.usu.edu/apps/doc/A605914233/AONE?u=utah_gvrl&sid=AONE&xid=61c2cb34.

[70] "Diplomacy and Dividends: Who Really Controls the Wagner Group?" Foreign Policy Research Institute. Accessed December 11, 2019. https://www.fpri.org/article/2019/10/diplomacy-and-dividends-who-really-controls-the-wagner-group/.

[71] Bennett, , 2012.

[72] Olsen, Deidre. "How Memes Are Being Weaponized for Political Propaganda." Salon. Salon.com, February 24, 2018. https://www.salon.com/2018/02/24/how-memes-are-being-weaponized-for-political-propaganda/.

[73] Prosser, Michael B. Memetics—a growth industry in US military operations. MS Thesis, School of Advanced Warfighting, United States Marine Corps, 2006. Retrieved from www.dtic.mil/dtic/tr/fulltext/u2/a507172.pd

[74] Gerasimov, 2013.

[75] Hodges, Doyle, P.W. Singer, and Emerson T. Brooking. "Like War: The Weaponization of Social Media." *Naval War College Review* 72, no. 3 (2019).

[76] Ibid.

[77] "Removing More Coordinated Inauthentic Behavior From Russia." About Facebook.

[78] "Exposing Russia's Effort to Sow Discord Online." U.S. House of Representatives Permanent Select Committee on Intelligence.

[79] Ibid.

[80] Ibid.

[81] Linvill, 2019.

[82] US House of Representatives Permanent Select Committee on Intelligence. Accessed December 10, 2019. https://intelligence.house.gov/uploadedfiles/hpsci_minority_exhibits_memo_11.1.17.pdf.

[83] Exposing Russia's Effort to Sow Discord Online." U.S. House of Representatives Permanent Select Committee on Intelligence

[84] "Assessing Russian Activities and Intentions in Recent US Elections." Office of the Director of National Intelligence. 2017. p. 3

[85] Helbing, Dirk. "Will Democracy Survive Big Data and Artificial Intelligence?" Scientific American, February 25, 2017. https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/.

[86] U.S. Congress. Senate. Select Committee on Intelligence. *Statement for the Record, Worldwide Threat Assessment of the U.S. IC*. By Daniel R. Coats. 116th Cong., 1st sess. S. Washington, DC: Office of the Director of National Intelligence, 2019. 7.

[87] Shao, Grace. "Fake Videos Could Be the next Big Problem in the 2020 Elections." CNBC. CNBC, October 15, 2019. https://www.cnbc.com/2019/10/15/deepfakes-could-be-problem-for-the-2020-election.html.

[88] "Gabon President Ali Bongo 2019 New Years Message." YouTube. Google LLC, December 31, 2018. https://www.youtube.com/watch?v=YABdm-12PQo.

[89] "Gabon's Ali Bongo Suffered a Stroke, Says Vice-President." BusinessLIVE. Business Day. Accessed October 10, 2019. https://www.businesslive.co.za/bd/world/africa/2018-12-09-gabons-ali-bongo-suffered-a-stroke-says-vice-President/.

[90] "Gabon's Government Quashes Coup Attempt, Killing 2, Officials Say | CBC News." CBCnews. CBC/Radio Canada, January 7, 2019. https://www.cbc.ca/news/world/gabon-coup-attempt-1.4968177.

[91] "I Was in Bed with Minister, Confesses Man Claiming to Be in Viral Sex Clip." Malaysiakini. Malaysiakini, June 11, 2019. https://www.malaysiakini.com/news/479268.

[92] Chia, Rachel Genevieve. "'My Loyalty Has Its Limits', Azmin Says after Investigation Results, While Anwar Claims the Pair Are 'Still a Team'." Business Insider Singapore, July 22, 2019. https://www.businessinsider.sg/my-loyalty-has-its-limits-azmin-says-after-investigation-results-while-anwar-claims-the-pair-are-still-a-team/.

[93] Windrem, Robert, and Ben Popken. "Russia's Propaganda Machine Discovers 2020 Democratic Candidate Tulsi Gabbard." NBCNews.com. NBCUniversal News Group, February 11, 2019. https://www.nbcnews.com/politics/2020-election/russia-s-propaganda-machine-discovers-2020-democratic-candidate-tulsi-gabbard-n964261.

[94] "Russia's Media Mentions of 2020 Democratic Candidates." Foreign Policy Research Institute. Accessed December 10, 2019. https://www.fpri.org/fie/russia-media-mentions/.

[95] Ibid.

[96] Ibid.
[97] Plouffe, David, “Hillary Clinton,” October 17, 2019, in *Campaign HQ with David Plouffe*, podcast, MP3 audio, 35:47, https://www.radio.com/media/audio-channel/hillary-clinton.
[98] Tulsi Gabbard (@TulsiGabbard), “Great! Thank you @HillaryClinton. You, the queen of warmongers, embodiment of corruption, and personification of the rot that has sickened the Democratic Party for so long, have finally come out from behind the curtain. From the day I announced my candidacy, there has been a,” Twitter, October 18, 2019, 2:20 p.m., https://twitter.com/TulsiGabbard/status/1185289626409406464
[99] Stracqualursi, Veronica. “'I Am Not a Russian Spy': Jill Stein Slams Clinton's Accusations.” CNN. Cable News Network, October 19, 2019. https://www.cnn.com/2019/10/19/politics/jill-stein-responds-clinton-gabbard-russian-asset-cnntv/index.html.
[100] “Removing More Coordinated Inauthentic Behavior From Iran and Russia.” About Facebook, November 13, 2019. https://about.fb.com/news/2019/10/removing-more-coordinated-inauthentic-behavior-from-iran-and-russia/.
[101] Mazarr, p. 60.
[102] Conger, Kate. "Twitter Says It's Banishing Political Ads." *New York Times*, October 31, 2019, A1(L). *Gale Academic Onefile* (accessed December 10, 2019). https://link-gale-com.dist.lib.usu.edu/apps/doc/A604285365/AONE?u=utah_gvrl&sid=AONE&xid=bd8cdd82.
[103] Dailymail.com, Marlene Lenthang For. “Russian Trolls Share 'Trojan Horse' Uplifting Tweets before Planting Distrust Ahead of 2020 Election.” Daily Mail Online. Associated Newspapers, November 26, 2019. https://www.dailymail.co.uk/news/article-7724925/Russian-trolls-share-Trojan-horse-uplifting-tweets-planting-distrust-ahead-2020-election.html.
[104] Ibid.
[105] “2019 Global Threat Report: Adversary Tradecraft and the Importance of Speed.” crowdstrike.com. George Kurtz, CEO. Accessed December 4, 2019. https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2019GlobalThreatReport.pdf.
[106] Polantz, Katelyn, and Stephen Collinson. “12 Russians Indicted in Mueller Investigation.” CNN. Cable News Network, July 14, 2018. https://www.cnn.com/2018/07/13/politics/russia-investigation-indictments/index.html.
[107] Mueller, 2019.
[108] Murray, Sara, and Lindsay Benson. “Maria Butina Released from Federal Prison, Deported to Russia.” CNN. Cable News Network, October 25, 2019. https://www.cnn.com/2019/10/25/politics/maria-butina-released/index.html.
[109] Nakashima, Ellen. "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms." *Washingtonpost.com*, February 26, 2019. *Gale Academic Onefile* (accessed December 10, 2019). https://link-gale-com.dist.lib.usu.edu/apps/doc/A576023957/AONE?u=utah_gvrl&sid=AONE&xid=09a43ba0
[110] Barnes, Julian E. "Cyberattack Neutralized Russian Trolls As U.S. Voted." *New York Times*, February 27, 2019, A9(L). *Gale Academic Onefile* (accessed December 10, 2019). https://link-gale-com.dist.lib.usu.edu/apps/doc/A576011132/AONE?u=utah_gvrl&sid=AONE&xid=00f8d934.
[111] Conley, Heather A. “Successfully Countering Russian Electoral Interference.” Successfully Countering Russian Electoral Interference | Center for Strategic and International Studies, June 21, 2018. https://www.csis.org/analysis/successfully-countering-russian-electoral-interference.
[112] “Removing More Coordinated Inauthentic Behavior From Russia,” 2019.
[113] Ibid.