The Dark Arts of Deception: What's Old? What's New? What's Next?

Global Populisms Conference
March 1-2, 2019

Amy Zegart
Stanford University

Abstract: This memo seeks to put Russia's current information warfare efforts into broader context by asking, "What's old? What's new? What's next?" Although leaders have been using deception operations and peddling false information across borders for centuries, two significant changes appear to be in the offing: (1) Deception efforts are now able to effectively target masses, not just elites; (2) Information warfare is likely to get much worse with advances in Artificial Intelligence-enabled fake audio and video.

Russia's operation to influence the 2016 American presidential election is a watershed moment that signifies both change and continuity in the dark arts of deception.[1] By now, the story is well known, though the details grow worse with time. In January 2017, the U.S. Intelligence Community concluded with "high confidence" that the operation was ordered by Russian President Vladimir Putin to "undermine public faith in the U.S. democratic process" as well as denigrate Democratic candidate Hillary Clinton and help elect Republican candidate Donald Trump.[2] The operation was multi-faceted. It included hacking into election-related accounts and disseminating stolen information through Wikileaks, attempting to penetrate more than a dozen state and local voting systems, amplifying messages with state-supported propaganda outlets like RT, and most importantly, weaponizing social media against American citizens.

We now know that the Internet Research Agency (IRA) – a "troll farm" based in Saint Petersburg with close ties to Putin – created thousands of fake social media accounts on Facebook, Twitter, Instagram, and YouTube, controlled by both Russians and bots, to impersonate Americans in order to spread pro-Trump and anti-Clinton sentiments and create general political discord and confusion.[3] Ongoing investigations by the social media companies and the U.S. government have uncovered a larger-scale operation than previously understood:

[1] Terms such as influence operations, information warfare, propaganda, active measures, disinformation, and deception are loosely used in both academic and popular discourse. In some instances, for example, the information conveyed may be true, but a state's role in disseminating that information is deliberately obscured. Others distinguish between the tactical use of deceptive information in warfare to protect troop movements (such as Operation Double Cross which enabled the Allies' surprise D-Day landing at Normandy) and the strategic use of deceptive information to gain geopolitical advantage during times of peace (such as Soviet Maskirova during the Cuban missile crisis). This memo examines deception broadly defined as the use of *knowingly false* information with the intent to deceive a receiving party. My interest lies chiefly in the use of deception by states across borders, though it is worth noting that the use of half-truths and outright lies has a storied history in domestic American political campaigns. See for example, Jill Lepore, *These Truths: A History of the United States* (New York: W.W. Norton, 2018).

[2] Assessing Russian Activities and Intentions in Recent US Elections," Intelligence Community Assessment, ICA 2017-01D, January 6, 2017, p. ii.

[3] Martin Matishak, "What we know about Russia's election hacking," *POLITICO,* July 18, 2018, https://www.politico.com/story/2018/07/18/russia-election-hacking-trump-putin-698087.

- Twitter has now found more than 3,800 accounts controlled by Russians and 50,000 suspected Russian "bots"—accounts that automatically generated 2.1 million election-related tweets receiving 454.7 million impressions during the final 10 weeks of the 2016 presidential election.[4]
- Google has discovered that suspected Russian agents uploaded more than 1,000 YouTube videos about divisive social issues.[5]
- Facebook has revealed that Kremlin-instigated content may have reached as many as 126 million Americans, more than a third of the U.S. population.[6]
- Senate Intelligence Committee chairman Richard Burr even had his own Cuban missile crisis moment during a November 1, 2017 hearing—bringing out the big posters to show smoking gun evidence of Russian duplicity.[7] Instead of secret missile sites, his pictures displayed two popular Facebook groups: Heart of Texas and United Muslims of America. Both were conjured up by Russia's deceptively named "Internet Research Agency" to lure hundreds of thousands of American followers. On May 21, 2016, both IRA-front sites organized protests outside the same Houston mosque at the same time – one to "Stop Islamization of Texas," the other to "Save Islamic Knowledge" protest. The result: angry protests pitting real Americans against each other on the streets of Houston, all instigated by the Kremlin.

Russia's playbook isn't just for Russians anymore. A number of Israeli companies staffed by former intelligence officers have engaged in information warfare-for-hire, using false identities, fake social media accounts, dummy Gmail accounts, and other tools to spread messages with the intent of influencing what people believe even if it isn't true. One of these companies, Psy-Group, created a brochure that featured a goldfish with a shark fin on its back below the tagline, "Reality is a matter of perception." Its alleged activities have included everything from creating a sham European think tank that churned out reports favoring the parliamentary election campaign of a client, to creating web sites making false claims disparaging the opponent of a client running for

[4] "Update on Twitter's review of the 2016 US election," Blog Post, Twitter, January 19, 2018, https://blog.twitter.com/official/en_us/topics/company/2018/2016-election-update.html; Gerrit De Vynck and Selina Wang, "Russian Bots Retweeted Trump's Twitter 470,000 Times," *Bloomberg,* January 26, 2018, https://www.bloomberg.com/news/articles/2018-01-26/twitter-says-russian-linked-bots-retweeted-trump-470-000-times.

[5] Kent Walker, Testimony before Senate Select Committee on Intelligence, *Social Media Influence in the 2016 US Elections* (115th Cong., 1st sess.), November 1 2017, https://www.intelligence.senate.gov/sites/default/files/documents/os-kwalker-110117.pdf.

[6] Colin Stretch, Testimony before Senate Select Committee on Intelligence, *Social Media Influence in the 2016 US Elections* (115th Cong., 1st sess.), November 1 2017, https://www.intelligence.senate.gov/sites/default/files/documents/os-cstretch-110117.pdf.

[7] Exhibit from Senate Select Intelligence Committee, Hearing, *Social Media Influence in 2016 U.S. Elections*, (115th Cong., 1st sess.), November 1, 2017, https://www.intelligence.senate.gov/sites/default/files/documents/Exhibits%20used%20by%20Chairman%20Burr%20during%20the%202017-11-01%20hearing.pdf.

the local hospital board in Tulare, CA, a town of just 60,000.[8] These activities appear to be legal. As former senior Israeli intelligence official Uzi Shaya put it, “Social media allows you to reach virtually anyone and to play with their minds….You can do whatever you want. You can be whoever you want. It’s a place where wars are fought, elections are won, and terror is promoted. There are no regulations. It’s a no-man’s land.”[9]

American domestic political players have gotten into the deception game, too. In late 2018, news surfaced that Democratic political operatives were behind at least two “false flag” social media campaigns designed to discredit Republican Alabama Senate candidate Roy Moore in his 2017 special election bid against Democrat Doug Jones. One operation used online accounts to make it look like Moore was supported by the Russians. He wasn’t. The second linked Moore to “Dry Alabama,” a fake online group – with a Facebook page and Twitter account – that said it prayed for Moore, spurned alcohol as “the devil’s tonic,” and supported a statewide liquor ban. Dry Alabama wasn’t real, either. It was a fiction conjured by Democratic operatives to peel moderate Republican votes from Moore to Jones. Although the operations appear to have been conducted without the knowledge or approval of Jones, who has called for a Federal Election Commission investigation,[10] the implications are serious: Ever since the 2016 presidential election, experts have been warning that it wouldn’t be long before domestic political groups copied the Russian playbook, using new technologies to spread disinformation, sow distrust, and widen social cleavages in a tight electoral race. They were right.

These recent developments suggest the weaponization of social media to spread false content for political gain is not going away any time soon. Examining how these emerging tools fit into the history of geopolitical deception is important for understanding the past, assessing the present, and defending democracies in the future.

What’s Old?

Deception is as old as warfare. In 480 B.C. an Athenian general named Themistocles used a double agent to lure the Persian navy into the narrow Strait of Salamis, where it was ambushed and defeated by a smaller fleet of more maneuverable

[8] Adam Entous and Ronan Farrow, “Private Mossad for Hire,” *The New Yorker*, February 11, 2019, https://www.newyorker.com/magazine/2019/02/18/private-mossad-for-hire.

[9] Quoted in Entous and Farrow, “Private Mossad for Hire.”

[10] Scott Shane and Alan Blinder, “Secret Experiment in Alabama Senate Race Imitated Russian Tactics,” *The New York Times,* December 19, 2018, https://www.nytimes.com/2018/12/19/us/alabama-senate-roy-jones-russia.html; Alan Blinder, “Doug Jones Seeks Inquiry Into Misinformation Efforts in Alabama Senate Race, *The New York Times,* January 9, 2019, https://www.nytimes.com/2019/01/09/us/doug-jones-alabama-senate.html; Craig Timberg, Tony Roman, Aaron C. Davis, and Elizabeth Dwoskin, “Secret Campaign to use Russian-inspired tactics in 2017 Ala. Election stirs anxiety for Democrats,” *The Washington Post,* January 6, 2019, https://www.washingtonpost.com/business/technology/secret-campaign-to-use-russian-inspired-tactics-in-2017-alabama-election-stirs-anxiety-for-democrats/2019/01/06/58803f26-0400-11e9-8186-4ec26a485713_story.html?utm_term=.78680b254952; Scott Shane and Alan Blinder, “Democrats Faked Online Push to Outlaw Alcohol in Alabama Race,” *The New York Times,* January 7, 2019, https://www.nytimes.com/2019/01/07/us/politics/alabama-senate-facebook-roy-moore.html.

Greek ships. The Battle of Salamis was one of the most consequential naval victories in recorded history.

America's founding also owes much to deception – on the battlefield as well as in the court of public opinion. As commander-in-chief of the Continental Army, George Washington made extensive use of espionage and deception to protect his troops, trick British forces, and avoid more battles than he fought; his military strategy was to outsmart the enemy, not outfight him. In 1775, for example, with his munitions dangerously low, Washington ordered fake gunpowder casks be filled with sand and shipped to depots where he knew they would be spotted by British spies. During the now-famous Valley Forge winter of 1777–78, as his troops were starving, freezing, and dying, Washington penned fake documents referring to phantom infantry and cavalry regiments to convince British General Sir William Howe that the rebels were too strong to attack. It worked. Had Howe known the truth and pressed his advantage, the Continental Army might not have survived the winter.[11]

Benjamin Franklin, for his part, waged influence operations in Europe to secure public and elite support for the American war effort. A printer by trade, Franklin set up a printing press in his Paris basement which churned out articles designed to sway European opinion. Some of his "news stories" were complete fabrications. In one, he penned a fake letter from a German prince to the commander of Prussian mercenary forces fighting for the British which advised the commander to let his wounded troops die since the British paid more for a dead solider than a wounded one. The letter generated protests in Britain and desertions among Prussian troops in the colonies. In another, Franklin printed a fake Boston newspaper replete with fake local news and even fake local advertisements. The main "story" involved a letter from an officer of the New England militia claiming the British royal governor of Canada was paying Indian allies for American scalps of women and children. The story was picked up in Britain and used by Whig opponents of the war. For Franklin, no detail was too small; he imported European paper and type to make his documents look more authentic. Two centuries later, the Central Intelligence Agency honored Franklin as a Founding Father of American Intelligence.[12]

Russia's 2016 social media operations in particular have deep historical roots; Russians have long used deception across borders to try to influence perceptions.[13] Disinformation campaigns were considered so important during the Cold War, they were

[11] Amy Zegart, "George Washington was a Master of Deception," *The Atlantic*, November 25, 2018, https://www.theatlantic.com/ideas/archive/2018/11/george-washington-was-master-deception/576565/.

[12] P.K. Rose, *The Founding Fathers of American Intelligence* (Washington, D.C.: Central Intelligence Agency, 1999), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/the-founding-fathers-of-american-intelligence/art-1.html.

[13] The Soviets have also waged campaigns that used truthful, though often exaggerated, information to inflame existing divides. Many of these efforts have focused on racial tensions in the United States. See for example Julia Ioffe, "The History of Russian Involvement in America's Race Wars," *The Atlantic*, October 21, 2017, https://www.theatlantic.com/international/archive/2017/10/russia-facebook-race/542796/.

placed under the command of a KGB general.[14] Soviet strategies included sending forged documents to legitimate news outlets so that they could gain both circulation and credibility. Congressional testimony from CIA officials and publicly available sources from the 1960s to the 1980s reveal that more than 80 forged American documents were created as part of Soviet disinformation efforts that were detected by the United States.[15] These included a forged telegram meant to be distributed to the Pakistani press which tried to tie the killing of Afghan leader Hafizullah Amin to a CIA plot,[16] and Operation INFEKTION, an operation to spread the false narrative that AIDS was created by United States government biological weapons experiments – which started with a fake anonymous letter from an American scientist to an Indian newspaper.[17]

What's New? And What's Next?

The use of deception may be old, but technology is changing the deception game in two important ways. The first is reach. For most of history, deception was largely an elite affair, designed by some leaders to trick other leaders. The Allies' surprise D-Day landing, for example, hinged on convincing Hitler and his top military commanders that Pas-de-Calais was the planned invasion site, not Normandy. To secure the advantage of surprise, the allies staged the most successful deception operation in history. It included turning nearly all of Germany's spies into unwitting double agents and feeding them false information about invasion plans, as well as inventing a fictitious army called the First United States Army Group which was led by Lieutenant General George Patton and included dummy landing craft, fake oil storage depots, and more—all to convince any German observers or aerial reconnaissance that the phantom force was real. Hitler was so thoroughly deceived, he delayed sending reinforcements to Normandy even

[14] Dennis Kux, "Soviet Active Measures and Disinformation: Overview and Assessment," *Parameters*, Vol. XV, No. 4 (Winter 1985), p. 20.

[15] Kux, p. 24.

[16] Kux, p. 24, citing House Permanent Select Committee on Intelligence, Hearing, *Soviet Active Measures*, (97th Cong., 2d session) July 13-14, 1982, p. 90, https://books.google.de/books?id=yWDHhvlvNZoC&printsec=frontcover&hl=de&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false. See also U.S. Department of State, "Soviet Active Measures: An Update," *Special Report 101* (July 1982), http://insidethecoldwar.org/sites/default/files/documents/Department%20of%20State%20report%20Soviet%20Active%20Measures%20Update%20July%201982.pdf; Ashley Deeks, Sabrina McCubbin, Cody M. Poplin, "Addressing Russian Influence: What Can We Learn From U.S. Cold War Counter-Propaganda Efforts?" *Lawfare*, October 25, 2017, https://www.lawfareblog.com/addressing-russian-influence-what-can-we-learn-us-cold-war-counter-propaganda-efforts.

[17] Thomas Boghardt, "Soviet Bloc Intelligence and its AIDS Disinformation Campaign," *Studies in Intelligence*, Vol. 53, No. 4 (December 2009), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no4/pdf/U-%20Boghardt-AIDS-Made%20in%20the%20USA-17Dec.pdf**;** Jasmine Garsd, "Long Before Facebook, the KGB Spread Fake News about AIDS," *National Public Radio*," August. 22, 2018, https://www.npr.org/2018/08/22/640883503/long-before-facebook-the-kgb-spread-fake-news-about-aids.

after the allies landed there because he was convinced it was a diversion, and the real invasion would still be at Pas-de-Calais.[18]

The most dangerous Cold War moment, the Cuban missile crisis, also featured deception operations targeting elites. This time, the United States was on the receiving end. The Soviets took extraordinary measures to hide their plans for deploying nuclear missiles in Cuba from everyone, even the Soviet ship crews carrying them.[19] Meanwhile, senior Soviet leaders publicly reassured President Kennedy and his advisors that Russia's military buildup in Cuba was purely defensive. They lied and Kennedy believed them.[20] It was only because CIA Director John McCone believed something nefarious must be afoot and insisted that U-2 spy planes be sent to photograph the Western part of Cuba, that Khrushchev's dangerous deception was discovered before all of his missiles became operational.[21]

Today, by contrast, deception is increasingly designed to trick millions of everyday citizens, not just a handful of top policymakers and elite opinion leaders. Already, half the world is online. By next year, more people worldwide are estimated to have mobile phones than running water or electricity.[22] Connectivity is spreading, and with it, the ability of false messages to "go viral" at scales and speeds that were previously impossible and unimaginable. In the 1980s, the Soviet Union's AIDS operation took several years to take hold and spread, one obscure newspaper story and conspiracy theorist at a time. Now, tweets and Facebook groups – especially incendiary ones -- can gain millions of views within hours. The Kremlin's state-funded media outlet RT (formerly Russia Today),[23] has a $300 million annual budget, broadcasts video programming that looks like legitimate news in multiple languages,[24] and has more than 3 million subscribers on YouTube – that's more than Fox News, CBS News or NBC News.[25] RT also has 2.71 million Twitter followers –four times the number of Twitter followers of the *Washington Post* White House Bureau Chief (Philip Rucker) and *New*

[18] Amy Zegart, "The Tools of Espionage are Going Mainstream," *The Atlantic*, November 27, 2017, https://www.theatlantic.com/international/archive/2017/11/deception-russia-election-meddling-technology-national-security/546644/.

[19] James H. Hansen, "Soviet Deception in the Cuban Missile Crisis," *Studies in Intelligence*, Vol. 64, No. 1, (Spring 2002).

[20] James M. Lindsay, "TWE Remembers: Andrei Gromyko Lies to John Kennedy," Council on Foreign Relations, October 18, 2012, https://www.cfr.org/blog/twe-remembers-andrei-gromyko-lies-john-kennedy-cuban-missile-crisis-day-three.

[21] Zegart, "The Tools of Espionage are Going Mainstream."

[22] CISCO, "10th Annual CISCO Visual Networking Index Mobile Forecast Projects 70 Percent of Global Population Will Be Mobile Users," February 3, 2016, https://newsroom.cisco.com/press-release-content?articleId=1741352.

[23]RT is described by the U.S. Intelligence Community as Russia's "principal international propaganda outlet" in "Assessing Russian Activities and Intentions in Recent US Elections," Intelligence Community Assessment, ICA 2017-01D, January 6, 2017, p. 13. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[24] Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model," RAND Perspective, 2016, p.2.

[25] Analysis of YouTube news subscribers by author. As of February 18, 2019, RT had 3.3 million subscribers, while Fox News had 2.5 million, CBS News had 1.2 million, and NBC News had 1.1 million. CNN and ABC News surpassed RT, with 6 million and 5.3 million subscribers, respectively.

York Times chief White House correspondent (Peter Baker) combined. As a recent RAND report noted, Russia has created a "disinformation chain" that reaches deep within targeted societies and consists of four key, often overlapping, links: (1) leadership from the Kremlin; (2) organs and proxies such as RT; (3) amplification channels such as social media platforms, fake and real accounts, bots, American news media, and unaffiliated websites that either intentionally or unintentionally amplify messages; and (4) consumers who spread the Russian narratives by retweeting, posting or promoting content.[26]

Second, technology is making deception much more sophisticated and harder to detect and counter. Russia's 2016 influence operation using Facebook and Twitter will look like the Flintstones compared to what's coming. Advances in artificial intelligence are fueling the development of "deep fake" digital impersonation technology that is diffusing widely. Already, commercial and academic researchers have created remarkably lifelike photographs of non-existent celebrities from whole cloth[27] as well as audios of people saying things they never uttered. Teams at Stanford University and the University of Washington have used AI and lip-syncing technology to generate deep fake videos, including demonstration videos of President Obama saying sentences he never actually said. While doctored images are nothing new, deep fakes are growing ever more convincing and nearly impossible to detect, thanks to a breakthrough AI technique invented by Google engineer Ian Goodfellow in 2014.[28] Called "generative adversarial networks," the approach essentially pits two computer algorithms against each other. One learns to generate a realistic image of something while the other learns to decide whether the image is real or fake. Because these algorithms are designed to learn by competing, deep fake countermeasures are unlikely to work for long. "We're in a fundamentally weak position," notes Hany Farid, a Dartmouth digital forensics expert.[29]

This technology is spreading, fast. In the last two years, anonymous GitHub user "torzdf" and Reddit user "deepfakeapp" have vastly simplified the code and interface required to generate deep fakes. Their programs, called "faceswap" and "FakeApp" have become easy enough to use that even a high school student with no coding background could make a deep fake with it. In addition to these models, generating sophisticated deep fakes requires access to two other key inputs: high-end computing power for machine learning such as graphics processing units (GPUs) or cloud-based computing, and large libraries of images to train algorithms. Both are becoming much more accessible. Anyone with a Google account can rent GPUs for as little as 13.5

[26] Elizabeth Bodine-Baron, Todd C. Helmus, Andrew Radin, and Elina Treyger, "Countering Russian Social Media Influence," RAND Report RR2740, 2018.

[27] Tero Karras, Timo Aila, Samuli Laine, Jaako Lehtinen, " Progressive Growing of GANS for Improved Quality, Stability, and Variation," NVIDA, ICLR paper 2018, https://research.nvidia.com/sites/default/files/pubs/2017-10_Progressive-Growing-of/karras2018iclr-paper.pdf.

[28] Martin Giles, "The GANfather: The man who's given machines the gift of imagination," *MIT Technology Review*, February 21, 2018, https://www.technologyreview.com/s/610253/the-ganfather-the-man-whos-given-machines-the-gift-of-imagination/.

[29] Ibid.

cents per hour, and the GitHub library "faceit" offers a program for creating deep fakes from any YouTube video.[30] Even without access to fancy GPUs or cloud computing services, any laptop could be used to create a deep fake, albeit one or two orders of magnitude more slowly.

The impact of deep fakes on deception could be profound, and policymakers know it. Just last month, deep fakes were a leading point of discussion at Congress's Worldwide Threat Hearings with American intelligence agency leaders.[31]

Anyone who has ever cried during a movie knows just how much video can manipulate human emotions. And that's when we know what we are seeing isn't real. Now imagine a world where a video depicts a foreign leader secretly discussing plans to build a clandestine nuclear weapons program or a parliamentary election candidate molesting a child just days before the election. Their denials are dismissed and the evidence seems incontrovertible because seeing has always been believing. Or imagine that someone creates fake photographs showing the families of American troops evacuating from South Korea—which North Korean leader Kim Jong Un mistakes as preparations for an American attack, so he launches a preemptive nuclear strike on Seoul. Lest anyone think that scenario might be far-fetched, think again. On September 21, 2017, with tensions between Washington and Pyongyang running high, someone actually did send fake text and social media messages ordering American military families and non-essential civilian personnel on the Korean peninsula to evacuate. U.S. Forces Korea had to issue a notification to ignore the fake "Official Alert."[32]

Deception has always been part of espionage and warfare, but not like this.

[30] "Faceit," Github, March 6, 2018, https://github.com/goberoi/faceit.

[31] Senate Select Committee on Intelligence, Hearing, *Hearing to Consider Worldwide Threats* (116th Cong., 1st sess.), January 29, 2019, https://www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats.

[32] Charlsy Panzino, "U.S. Force Korea: Evacuation messages is fake," *Military Times,* September 21, 2017, https://www.militarytimes.com/news/2017/09/21/us-forces-korea-evacuation-message-is-fake/; Zegart, "The Tools of Espionage are Going Mainstream."