alliance for securing democracy
G|M|F

Leaks, Lies, and Altered Tape

Russia’s Maturing Information Manipulation Playbook

Jessica Brandt, Head of Policy and Research
Amber Frankland, Research Assistant
October 14, 2020

Introduction

In 2016 the Russian government and its proxies interfered in the U.S. presidential election in a “sweeping and systematic” fashion.[1] Thanks to multiple bipartisan investigations and the work of researchers and journalists, rich detail about that operation—and the tools Russia’s disinformation agents used to execute it—are available to the public. In 2020 Americans are again preparing to elect a president. As the U.S. intelligence community assessed, and FBI Director Christopher Wray confirmed in recent testimony before Congress, Russia is conducting a “very active” interference campaign.[2]

Since 2016, Russia’s interference activity in the United States, and elsewhere around the world, has not abated. That’s because elections are a flashpoint for Russian information operations, but not the start or endpoint of this activity, which targets a broad range of polarizing or contentious political events. Over the past four years, the tactics, techniques, and procedures (TTPs) the Russian government and its proxies use to manipulate information and carry out deceptive campaigns have matured. These include:

- Co-opting authentic domestic voices and institutions, often by co-locating trolls within a target population, renting social media accounts of local actors, entrapping local leaders in “interviews” with purported journalists, recruiting real activists to foment protests, or mimicking or appropriating the names of local groups;
- Exploiting the anticipation of manipulation to claim that manipulation has occurred, often through false flag operations, or the amplification of homegrown conspiracy theories;
- Practicing tailored influence, by working through micro-influencers and in closed groups;
- Exploiting the full information ecosystem to launder a narrative, by seeding it with authentic domestic actors, deploying quasi-transparent Russian-supported media properties, and exploiting data voids.

Broadly speaking, we are witnessing a marked shift toward harder to detect, more targeted information operations that cover greater swaths of the information ecosystem, likely carried out by Russian military intelligence. That is a very different challenge than the one policymakers faced in 2016, when the threat was not yet fully comprehended, and in 2018, when the threat appeared to be largely driven by Internet Research Agency (IRA) trolls.

While it is important to glean lessons from those experiences, it is also important that policymakers not overlearn them, and in doing so, miss the consequential changes to Russia's information manipulation strategy that are now underway. These changes are occurring partly to evade increasingly sophisticated detection capabilities and policies on the part of social media platforms. But they are also occurring for a more fundamental reason: the Russian government and its proxies do not need to rely on large quantities of troll farm content to upend U.S. domestic politics with corrosive narratives that undermine trust in democratic institutions and belief in the existence of truth itself. The fire is already raging—it needs only a nudge here or there to be redirected to good effect.[3]

This paper is not meant to be a taxonomy of Russian TTPs generally, but to highlight evolving trends with relevance to policymakers. It is an effort to help stakeholders of all types—journalists, regulators, and researchers—look beyond individual campaigns to see the full picture of Russian activity as it is changing and to anticipate what might be to come.

Tactics, Techniques, and Procedures

Co-Opting Authentic Domestic Voices and Institutions

Russia and its proxy actors seek to co-opt legitimate domestic voices within target societies—particularly those of journalists and activists—for the purpose of disguising an operation as authentic advocacy. Among the favored techniques and procedures Russia and its proxies use for this purpose are co-locating trolls within a target population, renting social media accounts of local actors, and entrapping local leaders in "interviews" with purported journalists.

Co-Locating Trolls within a Target Population

In multiple instances, largely in Africa, Russian operatives have co-located trolls within the population they seek to target. For example, ahead of Madagascar's 2018 presidential election, more than 30 Russian agents were working inside the country. These operatives sought to influence the outcome of the election by publishing their own newspaper in the local language and hiring local students to write articles promoting positive narratives about the incumbent. They also paid local youth to attend rallies and hired journalists to cover those events, as well as recruited a cult leader to run in an attempt to split the opposition vote, among other lines of effort. According to operatives hired to take part in the campaign and internal documents viewed by The New York Times, the operation was ordered by Russian President Vladimir Putin himself, despite the fact that Madagascar has little obvious geopolitical value to Russia.[4] Its broad outlines are strikingly similar to the operation Russia carried out in the United States in 2016—namely, a disinformation campaign that aimed to sow division by splitting the opposition, supporting spoiler candidates, and fomenting offline protests. But the extent of the activity on the ground was much higher than it was during Russia's 2016 operation in the United States.[5]

Madagascar is not the only target of this technique. In October 2019, Facebook removed three Russian-backed influence networks aimed at several countries in Africa, including Cameroon, Central African Republic, Democratic Republic of the Congo, Libya, Mozambique, and Sudan. The networks were linked to Yevgeny Prigozhin, a Russian oligarch who was indicted by the United States in connection with Russia's interference in the 2016 U.S. presidential election through his leadership of the now-infamous troll farm the Internet Research Agency (IRA). In connection with the 2019 operation, Russians worked with in-country locals to create accounts disguised as authentic—an apparent effort to obviate the need to create accounts originating in Russia, suggesting an effort to improve operational security. Earlier IRA trolls were unmasked largely due to registration data (for example, IP addresses and phone numbers) that flagged inconsistencies with their stated locations. Setting up accounts within the target country allows these disinformers to better obfuscate their Russian connection. Posts connected with the operation promoted Russian policies and criticized French and American policies in Africa. One Facebook page purporting to be a news network called the Sudan Daily reposted articles from Russian state-backed media outlet Sputnik.[6]

These episodes demonstrate three key points. First, Russia's interference is multidimensional in nature. In the case of Madagascar, Russian operatives used multiple tools of interference in combination with one another—malign financial transactions, such as bribes; information manipulation; and cyber intrusions.[7] Second, Russia's information operations cross the full information ecosphere. They weaponize traditional media, including local media, which is often among the most trusted.[8] Third, activity that begins online does not stay there. As it did in 2016, Russia's information manipulation in the online space fomented protests in the streets.

Renting Social Media Accounts of Authentic Users

Russian actors have attempted to circumvent Facebook's safeguards by renting the accounts of genuine users in order to share content that appears authentic. For example, ahead of Ukraine's 2019 presidential election, authorities reported a Russian plot to pay Ukrainian citizens to give a Russian agent access to their personal Facebook pages, with the goal of using those accounts to publish political ads or plant fake articles.[9] Nina Jankowicz, a disinformation expert who has long studied Ukraine, conducted a Google search of "Facebook account rental" in Russian and Ukrainian that yielded numerous results. She found that various online platforms, including pages on Facebook itself, advertised that Facebook accounts active for more than six months and with at least 200 friends could earn the equivalent of one-third the average Ukrainian salary per month by giving an advertiser control of the account. She writes, "It's impossible to know the extent to which this practice has infiltrated Ukraine's political discourse, but the brazen attempts to recruit ad mules suggest it is a serious problem."[10]

Russia has a long history of using Ukraine as a testing ground for its active measures. But this operation, which was exposed shortly before voting day, evidences an evolution of technique—not least, an apparent effort to circumvent security measures put in place by the platform in the wake of 2016. The episode illustrates the interaction effect between foreign interference, domestic political activity, and the commercial market. There is a vibrant, for-profit market for Facebook account rentals, even though such activity is prohibited by Facebook's terms of service.[11] Exacerbating the problem, manipulation that happens off-platform is often difficult for platforms to detect.

Entrapping Local Leaders

In multiple campaigns targeting countries in what Russia calls its "near abroad," including Ukraine and Georgia, Russian military operatives used false personas to pose as journalists in order to conduct "interviews" with local leaders on politically sensitive subjects. The personas asked leading questions, inviting the target to make divisive comments, and then posted screenshots of the conversation to inflict political damage.[12] This is an evolution of earlier efforts by Russian hackers to pitch stolen materials to real journalists in order to solicit coverage—a tactic deployed against the Democratic party during the 2016 presidential election and the World Anti-Doping Agency after investigative reports revealed the extent of Russia's state-sponsored doping operation.[13] These episodes are emblematic of the shift to tailored influence, and of efforts to launder a narrative across the full information ecosystem (both tactics that are described in detail below). The private nature of direct messages between false personas and their targets make operations that happen in these forums more difficult to detect—yet another way Russian operatives are improving their operational security.[14]

Recruiting Domestic Activists to Create Protest Events

Russian actors have recruited authentic domestic activists to create protest events. For example, ahead of the 2018 U.S. midterm election, a Facebook group named "Resisters" organized at least 30 protest events that at least 40,000 people expressed interest in attending before they were removed for inauthenticity, which lawmakers and academics linked to Russia.[15] Disinformers used a false persona to recruit a legitimate, self-described anti-fascist activist to serve as an administrator of the page. The group billed itself as a feminist, anti-fascist community—one that ostensibly shared the activist's political goals. Subsequently, other administrators of the page created a protest event called "No Unite the Right 2," and began to invite other left-leaning groups to serve as co-hosts. One organizer noted that their fellow activist's status as an administrator "created a feeling of trust." More than 3,000 people indicated on Facebook that they planned to attend the event before it was removed.[16]

Stoking local protests is not a new tool. In 2016, the IRA used its Facebook presence to instigate real world events, including flash mobs, protests and rallies on American streets. More than 300,000 genuine users interacted with content promoting these events.[17] But in 2016, IRA actors created the pages and events. By 2018, Russian actors appear to have recruited real activists to do so, putting them out in front.

Mimicking or Appropriating the Names of Domestic Social Groups

Russian troll farm accounts have appropriated the names of authentic domestic social groups. In her analysis of a small set of IRA-linked Instagram accounts active in 2019, Young Mie Kim found that many accounts that engaged with 2020 election issues adopted the identities of domestic nonprofits in their messaging. Her research did not resolve whether the IRA was stealing names and logos in use by these groups, or whether it was "unwitting collaboration" between legitimate organizations and IRA shell groups.[18] Nonetheless, this effort marked a change from the IRA's 2016 tactics, which did not include the use of names or logos identical to those of existing organizations in its efforts to imitate them.[19]

Implications

The engagement of domestic voices and institutions in an information operation limits the response options available to platforms and governments. Most immediately, the involvement of citizens triggers constitutional protections around speech and assembly. In a broader sense, it impacts the political dynamics platforms and governments face. It is much easier to take down pages, groups, and accounts created by Russian trolls pretending to be local citizens than it is to do anything that might be seen to (or actually) restrict the speech of those citizens—even if they may have been coaxed by Russian actors. This is the case not least because Russian operators are skilled at targeting sympathetic agitators who already share their worldview. For both platforms and government, taking action in that context is politically fraught, not to mention damaging to the democratic principle of free expression.

Co-opting local actors also complicates detection efforts. It is challenging, if not impossible, for social media platforms to identify manipulative behavior when that behavior—for example, the solicitation of bribes—happens off-platform. Moreover, as Bret Schafer has noted, local actors may "be best positioned to recognize and ferret out the imposters in their midst," pointing out an example from 2016 in which Black Lives Matter activists identified what was revealed to be a fake, Russian-operated Facebook page due to its use of outdated language.[20] Co-opting local actors undermines this detection method.

The Kremlin's disinformation operators have used a handful of other tactics, techniques, and procedures to evade detection, which may be of relevance to policymakers. First, to avoid making obvious grammar, spelling, and syntax mistakes characteristic of 2016-era posts and advertisements, the IRA appears to be copying and pasting text from other sources. Second, troll farm operators appear to be using much less text and few hashtags in order to avoid detection from improved natural language processing programs. Third, IRA posts seem to remove or blur watermarks, also to evade detection.[21]

"Perception Hacking"

Since the exposure of Russia's "sweeping and systematic"[22] efforts to undermine the 2016 U.S. presidential election, Moscow has leveraged anticipation that election manipulation could occur to claim that it has, even in the absence of a successful campaign. Facebook's Head of Cybersecurity Policy Nathaniel Gleicher calls this trend "perception hacking," where small or questionably-effective networks seed the idea they are larger than they really are with the goal of sowing doubt.[23] The two primary techniques and procedures Russia relies on to conduct perception hacking are false flag operations and the amplification of homegrown conspiracy theories.

False Flag Operations

On the day of the 2018 U.S. midterm elections, a website that claimed to be run by Moscow's infamous Internet Research Agency (IRA) announced that it had conducted a successful, previously undetected influence campaign. Shortly before polls closed, the website published a list of fake Instagram accounts and a spreadsheet purporting to be the advance results of every Senate contest, and individuals connected with the website sent taunting messages to reporters in an unsuccessful effort to draw media attention to the campaign.[24] The episode built on an element of Russia's efforts to interfere in the U.S. presidential election in 2016: cyber intrusions into election systems in multiple U.S. states could have been an effort to lay the groundwork for a later information operation discrediting the outcome had the Kremlin's preferred candidate not won.[25]

The 2018 incident demonstrates that Russian TTPs are not evolving in isolation—platform, journalist, and civil society responses are changing too. It is a good reminder of the need for a whole of society approach that engages journalists—often a target of information operations[26]—as well as trusted researchers, in the effort to unmask foreign backed disinformation, including perception hacking efforts.

Amplification of Homegrown Conspiracy Theories

Russia also seizes on opportunities to promote domestic-origin conspiracy theories in target countries. For example, in the aftermath of the Iowa Caucus debacle, when the application intended to be used to report results malfunctioned, causing lengthy delays, Russian state media and diplomatic accounts seized the opportunity to sow chaos and doubt. In particular, they amplified false claims that the election had been rigged by the "corporate media" and Democratic party elites, as well as conspiracy theories around particular candidate ties to the malfunctioning app.[27] For example, the RT show "Going Underground on RT" questioned whether the delay in results was the result of "genuine irregularities or dirty tricks by the DNC."[28] RT's website, meanwhile, outlined what it described as "sordid details" about the funders of the malfunctioning app that allegedly "suggest[ed] a campaign to steal not just the election, but the party."[29] These ideas appeared to have domestic origins, and prominent U.S. political figures posted similar claims.[30]

The Iowa Caucus incident was of a piece with Russia's broader efforts to paint the Democratic primary as having been manipulated—a narrative it also pushed in 2016. For instance, in February of this year, following media reports that Russia-linked actors may have been supporting Senator Sanders' presidential campaign, Moscow sought to cast doubt on the allegations in part by claiming that they had been fabricated by "establishment Democrats" and the mainstream media to undermine the Senator's campaign. RT show "Redacted Tonight" went so far as to suggest the release of the reports was timed in an effort to inflict maximum damage on Sanders' campaign in the Nevada Caucus.[31]

These episodes demonstrate that Russia does not invent new narratives out of whole cloth, but rather draws on narratives that already exist—particularly those that undermine trust in elites and institutions. The more polarized the political climate in the United States becomes, the more fodder there is for this type of activity.

Implications

A perception hacking approach lowers the threshold for success—disinformers do not need to overcome platform detection capabilities or perpetuate an operation at scale to create the impression that they did (or to seize on confusion in the wake of a mishap, as in the case of the Iowa Caucus debacle). The approach also exposes the extent to which efforts to build resilience through public awareness must be carefully calibrated in order to avoid making the public more susceptible to claims of interference even when interference has not in fact taken place. More broadly, perception hacking complicates government efforts to unmask interference, particularly in an election context. Share too much and officials risk perpetuating the very notion they seek to dispel (that an election was compromised); share too little and they risk leaks of politicized or inconsistent information, which itself undermines faith in the electoral system. The Senate Select Committee on Intelligence's report on the U.S. Government Response Russian Activities illustrates the extent to which the Obama administration grappled with this dynamic in 2016.[32]

Practicing Tailored Influence

With increasing frequency, Russia's information manipulation efforts appear to target specific influencers (including local journalists and activists), rather than rely on large troll farms. The primary technique Russia deploys to implement this tactic is to work through micro-influencers and specific, often closed, Facebook groups.

Working through Micro-Influencers

Russian operatives have sought to gain the attention of authentic media influencers on various platforms. In February of this year, Facebook removed a network of pages, groups, and accounts linked to Russian military intelligence services, focused on Ukraine and its neighbors. The individuals posed as locals, and sometimes as citizen journalists, to contact journalists and other policymakers in the region. They also used these fake accounts to manage groups and pages, and to post and comment on content.[33] The individuals behind the operation created a presence across various blogging platforms that allow users to create new accounts easily. They then used different assets to amplify posts to specific audiences, including the Facebook groups.[34] This operation illustrates the cross-platform nature of the challenge, and the extent to which Russia's information operators seek to disguise themselves as legitimate domestic actors.

Last year, DFRLab researchers uncovered a large-scale influence operation, dubbed "Operation Secondary Infektion," that involved creating forgeries, turning them into memes, writing stories about them on various smaller platforms, and then amplifying those stories using Facebook accounts run from Russia. Individuals behind the operation posted content on platforms including Facebook, Twitter, Medium, and Reddit, as well as smaller sites like homment.com and indybay.org. The individuals behind the operation deployed consistent tradecraft. First, they would create an account and use it to post a false story. Then, they would deploy a second set of fake accounts to post expanded versions of the story in multiple languages, highlighting the original post as their source. Finally, they would deploy a third set of accounts to bring attention to the specific influencers: the traditional media.[35] These posts did not earn much traction, but that was likely not the point. As the DFRLab team notes, "This approach is suggestive of intelligence operators whose mission is to carry out their work undetected, without creating a discernible community," as opposed to content farms that aim to build as wide an audience as possible.[36] Again, the operation crossed multiple platforms, including small outlets. The individuals behind the operation used these platforms to launder their narratives across the information ecosphere.

Another operation, which, according to Graphika, strongly resembled "Operation Secondary Infektion" involved the leak of apparently unaltered U.K.-U.S. trade documents. The documents themselves were first published on Reddit before articles about the leaked documents appeared on smaller platforms. To draw attention to the leak, they tweeted the post directly to U.K. politicians and media figures and emailed it to political activists. Ultimately, they succeeded at making the news.[37] These operations were not hugely successful at drawing likes and retweets, but again, that was likely not their aim.

Targeting Specific (At Times, Closed) Groups

Russian actors have also directed their efforts at particular online groups. According to a BBC investigation, closed Facebook groups aimed at supporters of various U.K. political parties helped spread disinformation and polarizing content ahead of the 2019 European elections. The investigators found that pro-Brexit closed groups were a particular target for divisive content posted by users with foreign links, including at least one instance in which an apparently Russian user repeatedly posted links from pro-Kremlin disinformation outlet News Front. Content from conspiracy websites like Infowars and other sites that featured pro-Kremlin disinformation also formed part of this pattern.[38] Disinformers behind the Secondary Infektion and U.K. trade leaks operations also posted content to multiple political and news-focused groups in an effort to gain traction with particular populations.[39]

Implications

Working through micro-influencers and online groups is emblematic of a shift away from massive troll farms toward more targeted operations with the capacity to feed content into the traditional media ecosystem. This change in behavior may be a signal that Moscow has shifted toward greater Russian military intelligence involvement in its information manipulation operations, and away from reliance on content machines run by proxy actors, such as the IRA. And it underscores the importance of not over-learning the lessons of 2016 IRA operations, which had different goals and objectives and took on a different character than the interference we might expect in 2020 and beyond.

Laundering a Narrative Across the Full Information Ecosystem

Russia's ability to carry out successful information manipulation relies, as Kirill Meleshevich and Bret Schafer write, on creating "a fog of ambiguity between the Kremlin's actions and the Kremlin itself."[40] To do that, the Russian government works to create a facade of legitimacy by laundering information just as it might ill-gotten gains—placing, layering, and integrating them in ways that obscure their true origin.[41] The most common techniques and procedures Moscow uses to launder a narrative include seeding it with authentic domestic influencers in order to facilitate its spread across wide swaths of the information ecosystem, including offline; deploying quasi-transparent Russian government-supported media properties, including viral news video channels that are popular with young audiences on YouTube; and exploiting data voids to manipulate search results.

Seeding a Narrative with Authentic Domestic Actors

A prominent recent example of this technique is the "Ukraine did it" conspiracy theory, which asserts that Ukraine, and not Russia, interfered in the 2016 U.S. presidential election.[42] In an appearance before the House Intelligence Committee, former deputy assistant to the president and senior director for European and Russian affairs on the National Security Council Fiona Hill testified that, "This is a fictional narrative that is being perpetrated and propagated by the Russian security services themselves.[43] A closed intelligence briefing, which reportedly took place in fall 2019, informed senators that "Russia had engaged in a years-long campaign to essentially frame Ukraine as responsible for Moscow's own hacking of the 2016 election."[44] Nevertheless, numerous U.S. public officials, including the President of the United States, the Secretary of State, and at least one senator, appeared to bolster that claim, including on widely viewed television networks.[45]

According to data captured by the Hamilton 2.0 dashboard, Russian state media has amplified these claims. For instance, Sputnik published articles describing reports that former Trump campaign chairman Paul Manafort "blamed Ukraine rather than Russia" for the 2016 DNC server hack[46] and highlighted reports that President Trump "hated Ukraine for years" due to a belief that Ukrainians tried to help the Clinton campaign in 2016.[47] More glaringly, a Sputnik opinion piece outlined the CrowdStrike-Ukraine conspiracy theory in its entirety, suggesting that Russian hackers described in CrowdStrike's assessment of the 2016 DNC server hack were actually Russian speakers in Ukraine.[48]

The episode offers a reminder that disinformation spreads through various channels, both online and offline, including through domestic influencers and on television. It also highlights the fact that elections are a prominent, but not exclusive, flashpoint for Russia's information manipulation campaigns, which target a broad range of political events.[49]

Deploying Quasi-Transparent Russian Government-Supported Media Outlets

Russia uses quasi-transparent media properties to surface its narratives. One of these is Maffick Media, which in 2018 was a Berlin-based company running a network of media productions targeted toward young, digitally savvy, English-speaking audiences. The company's majority shareholder was Ruptly TV, a subsidiary of RT[50]—an affiliation that none of its social media accounts acknowledged until Facebook suspended several of the pages and asked the company to disclose this information for reinstatement.[51] The company has since re-registered as a limited liability company (Maffick LLC) in Delaware with a California subsidiary, according to California Secretary of State filings, and it no longer discloses a relationship with the Russian government on its social media accounts. However, a former RT employee remains listed as the manager in California, suggesting management continuity (though the current shareholding structure is unclear from the documents).[52] One of Maffick Media's brands, In the Now, is a viral news video channel with more than five million followers on Facebook.[53] The channel originated as a show on RT but became a standalone project in 2016.[54] In June, Facebook expanded its labeling of "state-controlled media," which applied to In the Now—a significant step toward transparency.[55] Seeking to evade the initiative, Maffick LLC filed a lawsuit in response, and a trial is now set for December 2020.[56]

Under the guise of independent journalism, these properties—part of Russia's propaganda network—target young, left-leaning Western audiences with slickly produced disinformation narratives that are, as Bradley Hanlon and Thomas Morley note, "packaged as meme-able satire and no-nonsense takes on history, environmental issues, and sensitive global politics."[57] This constitutes a shift in emphasis toward information manipulation in the quasi-overt, rather than fully covert, space. It also reflects an effort to shape the views of domestic influencers.

Exploiting Data Voids

"Data voids" occur when search engines have little natural content to return for a particular query.[58] In such cases, they are more likely to surface manipulated, conspiratorial, or otherwise problematic content because there is little else for search algorithms to return. Manipulators can use data voids to shape narratives around particularly sensitive topics by guiding users to search terms that they have co-opted, making it likely that users will see results that they have curated.[59]

Russia has used this technique in multiple contexts. For instance, a Russia-backed campaign to falsely label a volunteer humanitarian organization in Syria, the White Helmets, as terrorists exploited data voids and used other methods of algorithmic manipulation on search engines. At times, these tactics resulted in RT and Sputnik content pushing this narrative appearing among the top search results on Google and YouTube when users queried the organization.[60] Similar situations have occurred with topics such as the Skripal poisoning and the Nord Stream 2 pipeline[61]—all areas of particular geopolitical interest to Russia.

The technique only works on issue sets where there is a shortage of high quality content, and there is generally no such shortage on the substantive topics debated by the candidates during a presidential campaign. That said, the technique could be used going forward to mask interference using other asymmetric tools (for example economic coercion or malign finance) in cases where the historical record is thin, and therefore more vulnerable to manipulation.

Implications

Sophisticated information operations are not contained to the online space—they spread across respected media outlets, and even, at times, through domestic political figures. This diffusion can have a mutually reinforcing effect with efforts to amplify domestic conspiracy theories, including for false flag purposes. Moreover, the use of quasi-transparent media properties to spread particular narratives is emblematic of a shift toward the use of overt means of information manipulation. Ultimately, both exemplify Russia's efforts to engage multiple parts of the information ecosystem to surface the narratives it wishes to promote.

Feedback Loops

There are several feedback loops between these tactics, techniques, and procedures. For example, amplifying homegrown conspiracy theories can be a form of co-opting authentic domestic voices. And to the extent that such activity constitutes an effort to obscure the Kremlin's ties to a particular narrative, it can be a form of laundering information across the broader media ecosphere. Similarly, co-opting domestic voices, in particular journalists and social activists with substantial followings, can also be used as a means of conducting tailored influence—getting content seen by individuals likely to amplify it to key constituencies, including the traditional media. Likewise, there is a potentially reciprocal relationship between hack and leak operations and manipulation of the underlying media.

Conclusion

Since 2016, platforms have taken numerous steps to prevent the spread of Russian disinformation: enforcing new policies against coordinated inauthentic behavior, labeling state-funded media, requiring greater transparency and restrictions on advertising, and deploying fact-checkers are among them. Because of these changes, large social media operations run through content farms are now much easier for platforms to detect.

As a result, Moscow and its information operators are taking steps to overcome detection by improving their operational security, in part by deploying techniques that are less obviously manipulative. These techniques include:

- Co-opting authentic domestic voices and institutions, often by co-locating trolls within a target population, renting social media accounts of local actors, entrapping local leaders in "interviews" with purported journalists, recruiting real activists to foment local protests, or mimicking or appropriating the names of local groups;
- Exploiting the anticipation of manipulation to claim it has occurred, often through false flag operations, or the amplification of homegrown conspiracy theories;
- Practicing tailored influence, by working through micro-influencers and in closed groups; and
- Exploiting the full information ecosystem to launder a narrative, by seeding it with authentic domestic actors, deploying quasi-transparent Russian-supported media properties, and exploiting data voids.

These tools are used in combination with one another to carry out information campaigns that are more sophisticated, more targeted, and harder to detect than before. These campaigns cover large swaths of the information environment, including the offline space, and are likely to be carried out not by proxy trolls, but agents of military intelligence. That is a very different challenge than the one that caught policymakers flat-footed in 2016.

Changes in platform policies are not solely responsible for these shifts in Russia's strategy. This evolution is happening at least in part because Russia and its proxies do not need to rely on mass-produced troll farm content to upend U.S. domestic politics with destructive narratives that undermine trust in democratic institutions and the very notion of truth. As Laura Rosenberger has noted, "Putin's play is to throw a little accelerant on the fire occasionally and take advantage of our vulnerabilities."[62]

With the November 2020 election just ahead, at least three nightmare scenarios are on the horizon. The first is an information operation run through legitimate domestic actors—a scenario for which social media platforms are almost certainly unprepared. Platform policies take a hands-off approach to constitutionally protected speech of American citizens—as well they should. But disinformers are prepared to exploit this dynamic, weaponizing a strength and turning it into a vulnerability.

Much more thinking is needed about how to prevent disinformation that deliberately works through domestic actors without undermining essential freedoms that are themselves, like elections, institutions of democracy. In this endeavor, policymakers will face fraught tradeoffs and must remember not to lose the forest for the trees: the broader goal is to protect democracy, to which rights of expression are integral. That must come first.

A second nightmare scenario is a hack and leak of materials, some of which may be manipulated, potentially combined with a "perception hacking" effort. The Department of Homeland Security and the FBI warned U.S. states earlier this year that the threat of a hack and leak operation is "high."[63] Policymakers should prepare for an effort that implicates targets beyond candidates and their campaigns, or one designed to sow chaos in new ways. A hack and leak on a prominent journalist or news organization, for example, would pose particular challenges—not least if some of the released material is altered. That is because journalists would be called on to sort truth from fiction at the very moment that journalism is likely to face a crisis of trust. Such a scenario could be used to create the impression that there is no objective truth, or that the "corporate" media is "rigged"—themes that the Kremlin favors. Such a technique could be used to claim the existence of widespread manipulation, whether or not manipulation had occurred.

For democratic societies, making it through a hack and leak with trust in institutions reasonably intact may depend on how well its newsrooms handle the responsibility of reporting on potentially newsworthy information without inadvertently facilitating manipulation. That will require them to come up with guidelines for how they will deal with such a situation *in advance* of it arising—before the pressure of a scoop supersedes. Those guidelines should include a commitment to reporting on weaponized information in context, noting the source of the material and the motivations behind those who stole and released it.[64] Social media platforms have grappled with their role in facilitating the spread of content designed to polarize and mislead; media institutions must do the same.

A third nightmare scenario is a false flag operation capitalizing on confusion coronavirus-necessitated changes to voting processes may cause or the politicization of mail-in voting.[65] In September, the FBI and the Cybersecurity and Infrastructure Security Agency (CISA) issued a warning that possible delays in election tallies brought on by the pandemic may provide an opportunity for foreign actors to spread disinformation about the results.[66] They also warned about the potential for cyber actors to spread "false claims of hacked voter information" using "publicly available sources."[67]

Ultimately, political polarization is the single greatest obstacle to overcoming information manipulation—in part because it provides so much of the fodder for Russia's activities. Look no further than the "Ukraine did it" conspiracy theories that surfaced during President Trump's impeachment trial, the efforts to paint the 2020 primaries as rigged—throughout the process, and in particular after the Iowa Caucus debacle—or more recently, the amplification of divisive themes around race and policing.[68] Polarization also makes it more challenging for policymakers to take steps that would close vulnerabilities. Chief among those is ensuring that the public receives clear, apolitical messaging about Russia's disinformation activities. That clarity was lacking during the 2020 presidential primary, when the public instead received politicized leaks. Clear and consistent public messaging is crucial to maintaining public confidence in the integrity of the election system. So too is providing funding to the states, which actually run that system, in order to secure it—both physically, and from the possibility of becoming fuel for a false flag disinformation operation designed to undermine confidence in the legitimacy of the election outcome. Resourcing states will be particularly important in the context of the coronavirus epidemic, which has necessitated multiple changes to longstanding systems within a short time frame, potentially opening up space for confusion and mishaps that are bait for Russia's information manipulation.

Doubtless there are many other steps that need to be taken—not just by the federal government, but by social media platforms, political campaigns, state and local officials, journalists, and citizens. But the first step is almost certainly to develop a detailed understanding of the threat picture *as it stands now*, in order to anticipate what is to come.

Endnotes

1 Robert S. Mueller, III, Report on the Investigation into Russian Interference in the 2016 Presidential Election, Volume I of II, U.S. Department of Justice, 2019, p. 1.

2 William Evanina, "Statement by NCSC Director William Evanina: Election Threat Update for the American Public," Office of the Director of National Intelligence, August 7, 2020; Devlin Barrett, "FBI director affirms Russia's aim to 'denigrate' Biden ahead of election," The Washington Post, September 17, 2020.

3 William McKenzie, Lindsay Lloyd, and Christopher Walsh, "Democracy Talks: Laura Rosenberger, Alliance for Securing Democracy," George W. Bush Presidential Center, April 28, 2020.

4 Michael Schwirtz and Gaelle Borgia, "How Russia Meddles Abroad for Profit: Cash, Trolls and a Cult Leader," The New York Times, November 11, 2019.

5 According to the Special Counsel's report, two IRA employees traveled to the United States in 2014. See: Mueller, Report on the Investigation into Russian Interference in the 2016 Presidential Election, Volume I of II, p. 21.

6 Davey Alba and Sheera Frenkel, "Russia Tests New Disinformation Tactics in Africa to Expand Influence," The New York Times, October 30, 2019; Shelby Grossman, Daniel Bush, and Renée DiResta, "Evidence of Russia-Linked Influence Operations in Africa," Stanford Internet Observatory, October 29, 2019.

7 With respect to cyber operations, some of the Russian-run pages and groups used Facebook accounts that were stolen by hackers and repurposed. See: Alba and Frenkel, "Russia Tests New Disinformation Tactics in Africa to Expand Influence."

8 Andrew Guess, Brendan Nyhan, and Jason Reifler, "All Media Trust Is Local? Findings from the 2018 Poynter Media Trust Survey," Poynter Institute, August 10, 2018; Indira A. R. Lakshmanan. "Finally some good news: Trust in news is up, especially for local media," Poynter Institute, August 22, 2018.

9 Michael Schwirtz and Sheera Frenkel, "In Ukraine, Russia Tests a New Facebook Tactic in Election Tampering," The New York Times, March 29, 2019.

10 Nina Jankowicz, "Facebook's regulation fail in Ukraine should worry Europe," Politico, May 16, 2019.

11 Craig Silverman, "People Are Renting Out Their Facebook Accounts In Exchange For Cash And Free Laptops," Buzzfeed, January 18, 2019; Facebook, "Terms of Service," accessed October 13, 2020.

12 Ben Nimmo, Camille François, C. Shawn Eib, and L. Tamora, From Russia With Blogs: GRU Operators Leveraged Blogs, Social Media Accounts and Private Messaging to Reach Audiences Across Europe, Graphika, February 2020; Nathaniel Gleicher, "Removing Coordinated Inauthentic Behavior From Russia, Iran, Vietnam and Myanmar," Facebook Newsroom, February 12, 2020.

13 John Leicester, "Column: Shifting gears, Bears peddle hacked emails to media," Associated Press, December 24, 2016. In the case of the leaks, the perpetrators tampered with at least one document. Russian operatives have a pattern of altering the documents they leak for political purposes, as the investigations team Citizen Lab have documented. See: Raphael Satter, "Inside story: How Russians hacked the Democrats' emails," Associated Press, November 4, 2017; Adam Hulcoop, John Scott-Railton, Peter Tanchak, Matt Brooks, and Ron Deibert, Tainted Leaks: Disinformation and Phishing With a Russian Nexus, The Citizen Lab, May 25, 2017.

14 Julian E. Barnes and Adam Goldman, "Russia Trying to Stoke U.S. Racial Tensions Before Election, Officials Say," The New York Times, March 10, 2020.

15 Tony Romm and Elizabeth Dwoskin, "More than 40,000 Facebook users expressed interest in political protests with potential Russian ties," The Washington Post, August 8, 2018.

16 Tony Romm, Elizabeth Dwoskin, and Eli Rosenberg, "The moment when Facebook's removal of alleged Russian disinformation became a free-speech issue," The Washington Post, August 1, 2018.

17 U.S. Congress, Senate, Select Committee on Intelligence, Russian Active Measures, Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media with Additional Views, 116th Cong., 1st sess., 2019.

18 Young Mie Kim, "New Evidence Shows How Russia's Election Interference Has Gotten More Brazen," Bren-

nan Center for Justice, March 5, 2020.

[19] Ibid.

[20] Bret Schafer, "Race, Lies and Social Media: How Russia Manipulated Race in America and Interfered in the 2016 Elections," State of Black America, National Urban League, May 2019.

[21] Davey Alba, "How Russia's Troll Farm is Changing Tactics Before the Fall Election," The New York Times, March 29, 2020.

[22] Mueller, Report on the Investigation into Russian Interference in the 2016 Presidential Election, Volume I of II, p. 1.

[23] Fergal Gallagher, "Are Google, Twitter and Facebook doing enough to protect the 2020 election in the age of 'information disorder'?" ABC News, November 15, 2019.

[24] Ben Collins, "A Russian troll farm set an elaborate social media trap for the midterms — and no one bit," NBC News, November 7, 2018.

[25] U.S. Congress, Senate, Select Committee on Intelligence, Russian Active Measures, Campaigns and Interference, Volume 1: Russian Efforts Against Election Infrastructure with Additional Views, 116th Cong., 1st sess., 2019, p. 35-37.

[26] Bradley Hanlon, "Are Journalists Ready for Foreign Interference in 2020?" Alliance for Securing Democracy, November 7, 2019.

[27] Emily Birnbaum, "Iowa chaos highlights threat of domestic misinformation," *The Hill*, February 4, 2020; Rachel Dean Wilson, "Electability, Democracy, and the 2020 Primaries: What to Watch," German Marshall Fund of the United States, February 3, 2020; Amber Frankland and Bret Schafer, "Hamilton Weekly Report: February 1-7, 2020," Alliance for Securing Democracy, February 10, 2020.

[28] Frankland and Schafer, "Hamilton Weekly Report: February 1-7, 2020."

[29] RT, "Iowa disaster redux: DNC demands recanvass as more sordid details emerge about Shadow app's backers," February 6, 2020.

[30] Amanda Seitz and David Klepper, "Online conspiracy theories flourish after Iowa caucus fiasco," Associated Press, February 4, 2020.

[31] Jessica Brandt and Amber Frankland, "Hamilton Weekly Report: February 22-28, 2020," Alliance for Securing Democracy, March 2, 2020.

[32] U.S. Congress, Senate, Select Committee On Intelligence, Russian Active Measures, Campaigns, and Interference in the 2016 U.S. Election, Volume 3: U.S. Government Response to Russian Activities, 116th Cong., 2d sess., 2020.

[33] Gleicher, "Removing Coordinated Inauthentic Behavior From Russia, Iran, Vietnam and Myanmar."

[34] Nimmo, François, Eib, and Tamora, From Russia With Blogs.

[35] Nika Aleksejeva, Lukas Andriukaitis, Luiza Bandeira, Donara Barojan, et al., Operation "Secondary Infektion": A Suspected Russian Intelligence Operation Targeting Europe and the United States, DFRLab, August 2019.

[36] Ibid.

[37] Ben Nimmo, UK Trade Leaks: Operators keen to hide their identities disseminated leaked UK/US trade documents in a similar fashion to Russian operation "Secondary Infektion," exposed in June 2019, Graphika, December 2019.

[38] Marianna Spring and Lucy Webster, "European elections: How disinformation spread in Facebook groups," BBC, May 30, 2019; EUvsDisinfo, "No News on the News Front," April 29, 2019.

[39] Aleksejeva, Andriukaitis, Bandeira, Barojan, et al., Operation "Secondary Infektion"; Nimmo, UK Trade Leaks.

[40] Kirill Meleshevich and Bret Schafer, "Online Information Laundering: The Role of Social Media," Alliance for Securing Democracy, January 9, 2018.

[41] Ibid.

[42] There are three versions of this theory: that someone in Ukraine, and not Russia, hacked the Democratic

National Committee's network; that the cybersecurity firm CrowdStrike is Ukraine-based and that the DNC's server is in Ukraine; or that Ukraine interfered on behalf of Hillary Clinton. See: Thomas Rid, "Who's Really to Blame for the 'Ukraine Did It' Conspiracy Theory?" The Atlantic, December 5, 2019.

[43] U.S. Congress, House, Permanent Select Committee on Intelligence, "Impeachment Inquiry: Fiona Hill and David Holmes," November 21, 2019, p. 39-40.

[44] Julian E. Barnes and Matthew Rosenberg, "Charges of Ukrainian Meddling? A Russian Operation, U.S. Intelligence Says," The New York Times, November 22, 2019.

[45] Jessica Brandt, "The 'Ukraine did it' conspiracy theory is dangerous: Here's why," The Hill, December 2, 2019.

[46] Oleg Burunov, "Manafort Thought Ukraine, not Russia Hacked DNC Email Servers During 2016 Election Campaign – Report," Sputnik News, November 3, 2019.

[47] Sputnik News, "Trump 'Hated' Ukrainians for Years Over Their Alleged Conspiracy With Hillary Clinton – Report," November 3, 2019.

[48] Ekaterina Blinova, "Cyber Expert Explains the Theory of Crowdstrike's Connection to Ukraine, DNC Hacking Controversy," *Sputnik News*, September 27, 2019.

[49] Jessica Brandt, "Russian blame game sows U.S. discord to weaken Ukraine," Axios, November 23, 2019.

[50] Bradley Hanlon and Thomas Morley, "Russia's Network of Millennial Media," Alliance for Securing Democracy, February 15, 2019.

[51] Donie O'Sullivan, Drew Griffin, Curt Devine and Atika Shubert, "Russia is backing a viral video company aimed at American millennials," CNN, February 18, 2019.

[52] Casey Michel, "Russian-linked outlet fights Facebook transparency in U.S. courts," Eurasianet, August 27, 2020. See also: Casey Michel, Twitter post, April 26, 2020.

[53] Hanlon and Morley, "Russia's Network of Millennial Media." See also: In the Now's Facebook page, archived September 24, 2020.

[54] Ishmael N. Daro, "This Quirky New Viral Video Channel Is Funded By The Russian Government," Buzzfeed, December 15, 2016.

[55] Nathaniel Gleicher, "Labeling State-Controlled Media On Facebook," Facebook Newsroom, June 4, 2020. See also: Josh Rudolph and Thomas Morley, Covert Foreign Money: Financial Loopholes Exploited by Authoritarians to Fund Political Interference in Democracies, Alliance for Securing Democracy, August 2020, p. 92-93; Casey Michel, Twitter post, June 4, 2020.

[56] Michel, "Russian-linked outlet fights Facebook transparency;" David McAfee, "Facebook Avoids TRO in Suit Over Russian 'Controlled-Media' Tag," Bloomberg Law, August 27, 2020.

[57] Hanlon and Morley, "Russia's Network of Millennial Media."

[58] Michael Golebiewski and danah boyd, Data Voids: Where Missing Data Can Easily Be Exploited, Data & Society, October 29, 2019.

[59] Jessica Brandt, David Salvo, Lindsay Gorman, Bret Schafer, and Brenen Tidwell, "Ten Questions Lawmakers Should ask Tech Companies and Government Officials on Election Security," Alliance for Securing Democracy, May 22, 2019.

[60] Bret Schafer, "PD Next – De-Mystifying Disinformation, Malign Influence, and the Current Information Environment Session," Presentation at PD Next 2019 Conference, November 6, 2019. See also: Olivia Solon, "How Syria's White Helmets became victims of an online propaganda machine," The Guardian, December 18, 2017.

[61] Schafer, "PD Next."

[62] McKenzie, Lloyd, and Walsh, "Democracy Talks: Laura Rosenberger, Alliance for Securing Democracy."

[63] Eric Tucker, "US: Russia could try to covertly advise candidates in 2020," ABC News, May 4, 2020.

[64] Heidi Tworek, Responsible Reporting in an Age of Irresponsible Information, Alliance for Securing Democracy, March 2018.

[65] Jessica Brandt, "To Ensure a Healthy Election in a Pandemic, First Prepare the Information Space," Alliance for Securing Democracy, May 14, 2020.

[66] Maggie Miller, "FBI, DHS warn that foreign hackers will likely spread disinformation around election results," The Hill, September 22, 2020.

[67] Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, "Public Service Announcement: False Claims of Hacked Voter Information Likely Intended to Cast Doubt on Legitimacy of U.S. Elections," September 28, 2020.

[68] Matthew Rosenberg and Julian E. Barnes, "A Bible Burning, a Russian News Agency and a Story Too Good to Check Out," The New York Times, August 11, 2020; Amber Frankland, Etienne Soula, and Bret Schafer, "Hamilton Weekly Report: May 30-June 5, 2020," Alliance for Securing Democracy, June 9, 2020.