alliance for securing democracy
G|M|F

Policy Brief

2018 | No. 002

Online Information Laundering: The Role of Social Media

By Kirill Meleshevich and Bret Schafer

Revelations that the Kremlin exploited social networking tools to disseminate and promote divisive content in the United States and Europe have highlighted the role of those platforms in the proliferation of disinformation. While a great deal of attention has been given to both the creators and consumers of disinformation, far less focus has been paid to how disinformation spreads from questionable to credible sources online.

In order for social media companies to combat the misuse of their platforms by state and non-state actors, it is important to recognize how the online information space operates and what tactics are used by those exploiting it. Operational similarities between the placement and spread of disinformation online and the laundering of ill-gotten financial gains can provide useful insights for analysts and policymakers. By understanding those similarities, governments and the tech sector can fight disinformation by considering many of the techniques honed by anti-money laundering practitioners.

Want to combat disinformation? Borrow a page from the anti-money laundering handbook.

Russia's ability to successfully conduct hybrid warfare is predicated on the creation of a fog of ambiguity between the Kremlin's actions and the Kremlin itself. By conducting operations through an ad hoc network of proxies, carve-outs, and cutouts — whose connection to the Kremlin is difficult to definitively establish — the Russian government is able to maintain plausible deniability and thus lower the diplomatic and military costs of its actions. It is a strategy with deep roots: *maskirovka* — a Soviet-era military doctrine that translates as "mask" or "masquerade" — established operational deceit as a core tenet of both conventional and irregular warfare. While modern *maskirovka* is most commonly associated with the use of "little green men" to occupy Crimea, it is a tactic that is also deeply ingrained in the Kremlin's ongoing disinformation campaign against the United States and Europe. This presents an obvious challenge: How can the West respond to an adversary who denies even being present on the battlefield?

One answer may lie in understanding the operational resemblance between the spread of disinformation and the laundering of illicit funds. Just as ill-gotten money needs to be moved from an illegitimate source into an established financial institution, disinformation is most powerful when a façade of legitimacy is created through "information laundering." Anti-money laundering practitioners describe the need for financial criminals to place, layer, and integrate illicit funds, meaning that money obtained through criminal means needs

to find an entry point into the financial system, then move between banks or financial products to hide the identity of the owner, and finally be woven into an asset from which seemingly legitimate funds can be drawn. Russian disinformation follows a similar pattern; only here, the currency is information and the reward is influence. This piece will examine these similarities and explore the policy measures that could be taken in light of these findings.

Placement

Placement refers to the initial posting of misleading information on a website or social media account. Much like financial criminals establish certain types of bank accounts to deposit illicitly-obtained money into the banking system, disinformation campaigns selectively rely on certain social media accounts that can disseminate information in a manner that masks both its intent and its source.

In the money laundering context, this process is often achieved through the use of shell companies — firms with no physical location and little-to-no assets — because they are cheap to establish, provide anonymity, and can be jettisoned if their true purpose is revealed. Social media accounts offer disinformation campaigns the same benefits. They provide free access to a platform from which information can be spread, and in many cases the public account ownership need not have any link to the true owner.

A growing body of evidence, including testimony provided by technology companies to Congress in early November, has demonstrated how the Russian government sets up accounts on Facebook and Twitter, including those that appear to represent Tea Party groups, anti-immigration activists, faux social justice movements, and private citizens.[1] Account characteristics vary — from paid trolls operating sock puppets (fictitious online identities) to bots and cyborg accounts (human operated accounts that use automation to amplify their messaging). On Twitter, account names linked to the Kremlin-funded Internet Research Agency in St. Petersburg span a range of formats, including use of a generic Western name ("Sarah_Giaco"), a purported political leaning ("IMissObama"), an alleged affiliation with a news organization ("DallasTopNews"), a cultural reference ("30toMarsFandom"), or a single name followed by a string of numbers that sequentially change from one account to the next. Many of these accounts post identical or nearly identical information, often through the use of bots that are programmed to amplify and promote specific messages.

> *"Anti-money laundering practitioners describe the need for financial criminals to place, layer, and integrate illicit funds."*

While it is exceptionally easy to create hundreds of fictional online accounts, those accounts can be easily flagged as fraudulent by both Internet sleuths and social media platforms. Shell companies suffer from a similar dilemma: New accounts without a verifiable history often face greater scrutiny from banks and regulators. Financial criminals address this by using shelf companies, a variant that appears more legitimate because they were established years earlier, maintain some online presence (while still eschewing a physical presence), and may have been involved in some low volumes of legitimate activity. The Treasury Department in 2012 highlighted how a Swiss company established in 1999 was inactive until 2009, at which point it bought a bank in Belarus, setting off a chain of multibillion dollar financial transactions that "were indicative of money laundering."[2] The spread of disinformation online often relies on a similar technique. Fake social media accounts, available for purchase at bulk quantities through several websites, are more expensive if they are dated, meaning that they were established months or years before they are used to spread disinformation. These "aged" accounts are harder to identify as being part of a disinformation campaign because they may come with some previous user activity. An account that

1 The Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism. "Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions," October 31, 2017, https://www.judiciary.senate.gov/meetings/extremist-content-and-russian-disinformation-online-working-with-tech-to-find-solutions.

2 Department of the Treasury, "Finding That JSC Crdex Bank is Financial Institution of Primary Money Laundering Concern," May 25, 2012, Vol. 77, No. 102, https://www.gpo.gov/fdsys/pkg/FR-2012-05-25/pdf/2012-12742.pdf.

has a body of posts and re-posts, pictures of family and friends, and other "normal" activity becomes much harder to identify as a fake.

As with the shell company/social media bot analogy, investigative reporting has identified Russian government created Facebook pages that came with fabricated histories that were used to create an illusion of authenticity.[3] One striking example of a shelf account is that of Twitter handle @Jenn_Abrams, which was identified by Twitter in November 2017 as being linked to the Internet Research Agency. The account was originally established in 2014, routinely posted on a variety of political and apolitical topics, and garnered attention through divisive posts arguing about the need for race-based segregation among other incendiary topics. "Jenna Abrams" was a more effective channel to disseminate misleading and politically inflammatory information because of its shelf account characteristics, including apolitical postings, a body of followers, and an established account history. As a result, the account was often quoted and cited in various established publications. Additional media reporting from early November 2017 suggests that other such "shelf accounts" with ties to the Russian government were made active in the run up to the presidential election.[4]

While account structure is important, the manner by which information or funds are placed is also critical. In the realm of financial crimes, law enforcement cases in the United States and elsewhere routinely cite smurfing as an important step in the laundering process. Smurfing entails breaking up a pot of funds, say $100,000, into many smaller financial transfers that are more difficult to detect because they seem like legitimate retail transactions. A single $100,000 cash deposit or international wire transfer is easier for a bank to flag as questionable than 50 deposits of $2,000. Similarly, Russian disinformation efforts do not solely rely on a false message delivered through a single channel or medium. Instead, their efforts amount to "informational smurfing." During the 2016 U.S. presidential election, for example, the Russian government reportedly purchased thousands of targeted ads on Facebook and operated a yet-unknown number of accounts on both Facebook, Twitter, and Instagram (as of November 2017, 146 million Americans were potentially exposed to Russian government disinformation efforts). Disinformation was also spread through YouTube, Reddit, and a host of blogs and "news" sites, some with direct or indirect connections to Kremlin figures. The high volume of ads and posts made it difficult for fact-checkers to flag stories as misleading due to the fact that the original content was packaged and repacked by hundreds if not thousands of different accounts and websites. Informational smurfing thus provided a means to spread rumors in a fashion that was difficult to attribute and effectively debunk.

Layering

Layering is the process by which disinformation spreads from its point of origin to more credible sources, gaining credibility through reposts, likes, and shares. In anti-money laundering parlance, the term refers to the use of intermediary companies, banks, and individuals to send money across borders and through different types of financial products to break the chain between origin and beneficiary. These third party money launderers play a key role in successful money laundering operations, as evidenced by recent law enforcement cases that have highlighted how intermediaries move funds already placed into the financial system in order to provide additional distance from the originator.[5][6]

In disinformation campaigns, layering takes two forms. The first is use of middle-men who seemingly have no relation to the originator of the information. The second type of layering is through indirect citations (known as cascading citations) from unsubstantiated social media posts to seemingly legitimate news sources. The release of information pilfered from Democratic Party officials in mid-2016 provides a relevant example of the use of intermediaries. Rather than directly releasing Hillary Clinton campaign chairman John Podesta's hacked e-mails, the Russian government appears to have used

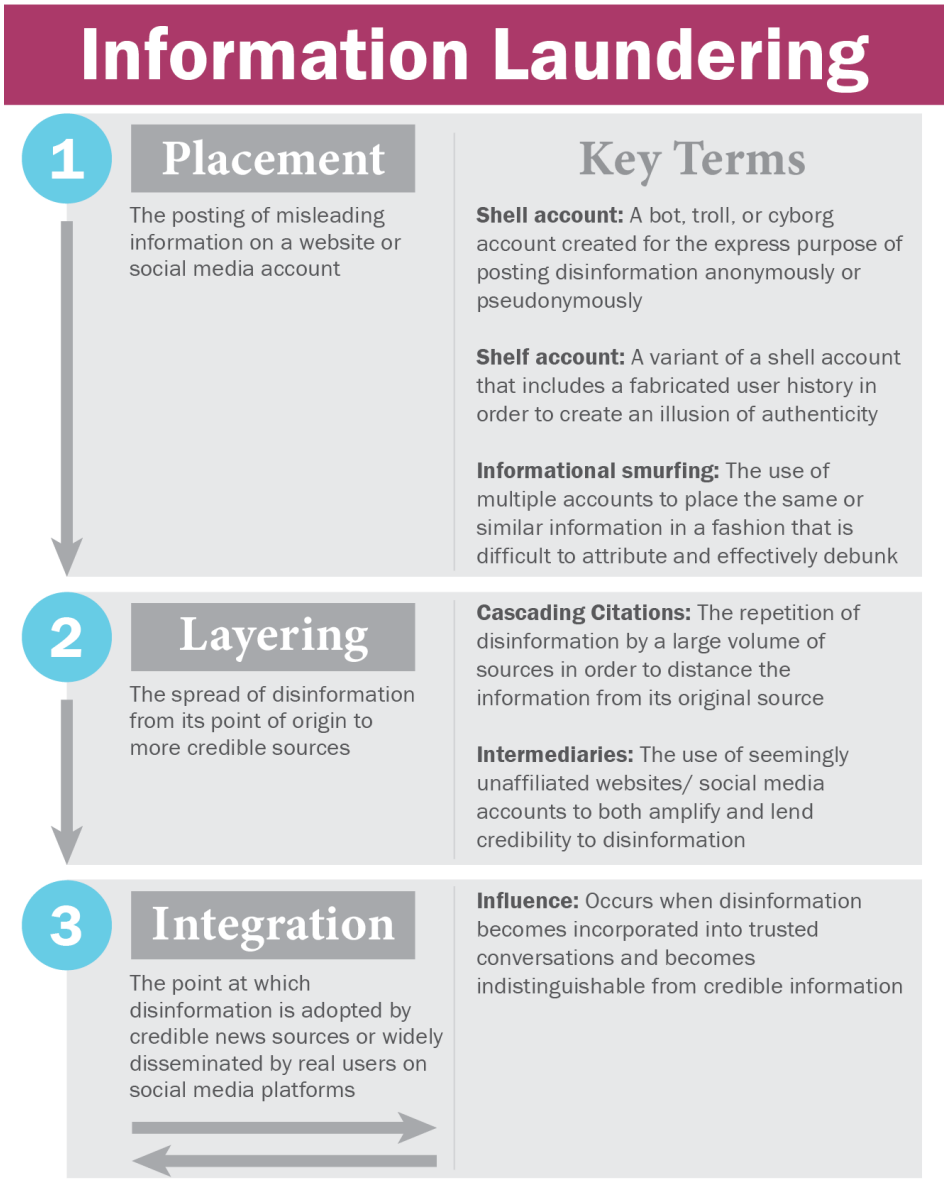
3 Scott Shane, "The Fake Americans Russia Created to Influence the Election," *The New York Times*, September 7, 2017.

4 Kevin Poulsen, "Exclusive: Russia Activated Twitter Sleeper Cells for 2016 Election Day Blitz," The Daily Beast, November 7, 2017.

5 U.S. Immigration and Customs Enforcement. "Third Party Money Launderers," The Cornerstone Report, Summer 2017, Vol. 8, No. 4, https://www.ice.gov/sites/default/files/documents/Report/2017/CSReport-13-4.pdf.

6 Department of the Treasury. "Notice of Finding That Banca Privada d'Andorra Is a Financial Institution of Primary Money Laundering Concern," March 6, 2015, https://www.fincen.gov/sites/default/files/shared/BPA_NOF.pdf.

several purported middle-men who instead released the information on their behalf. U.S. intelligence officials in early January 2017 expressed high confidence that Russian intelligence released Podesta's personal and professional e-mails through the Guccifer 2.0 and DCLeaks.com personas and indirectly through WikiLeaks.[7] These organizations benefited from the appearance of authenticity, and the release of information was not immediately attributed to an intelligence effort. The direct release of stolen personal communications of public officials on a Russian website would have been seen as a malicious attempt to influence a political outcome; it could also have been seen as potentially fabricated, and hence ignored. The use of intermediaries provided the information with a greater sense of legitimacy.



Organizations that purport to leak information as a public service are not the only intermediaries used in disinformation campaigns. As with money laundering operations, where banks and companies are sometimes unknowingly used as part of the layering processing, some individuals unwittingly spread misleading Russian government-generated information because it supports a political narrative, appears be real, or is simply viral in nature. This is evidenced by the revelation that a faux Black Lives Matter Facebook page connected to the Russian government attracted more than 300,000 likes,[8] many of them from legitimate users of the site who were unaware of its Russian links or fictitious nature. Authentic social media users can be duped into spreading false information in much the same way that a bank with an industry-leading compliance program can still facilitate money laundering; illegitimate funds and disinformation can sometimes be impossible to distinguish from legitimate activity.

Similarly, Jenna Abrams — the Twitter personality cited above that appears to have been set up as part of Russia's disinformation efforts — provided this same type of informational layering. That account served as a middleman both to spread inflammatory and misleading information and to create it through posts on Twitter and Medium. Because "her" account had

7 Office of the Director of National Intelligence. "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution." January 6, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

8 Jason Parham, "Russians Posing as Black Activists on Facebook is More than Fake News," *Wired*, October 18, 2017.

a large population of followers and had been quoted by a variety of print and online media outlets, it had a stronger veneer of legitimacy.

For money launderers, layering through intermediaries and other techniques is critically important because it creates friction in banks' and law enforcements' investigations and puts distance between the crime and the final destination of illicit funds. In select cases, disinformation online has been picked up by news outlets that are read and trusted by a large population of readers. Consider the case of Seth Rich, a Democratic National Committee staffer who was killed in Washington, DC. While online fact checkers debunked claims that his murder was linked to the release of DNC emails ahead of the 2016 presidential election, conspiracy theories surrounding his death were extensively covered by Russian government-sponsored media, including Russia Today and Sputnik.[9] Russia's Embassy in London even referred to Rich as a Wikileaks informant on a post to their official Twitter page. While the Embassy's Twitter page, RT, and Sputnik did not seemingly create the false information about Seth Rich, the dissemination of the false information through official social media sites provided a greater basis for others to accept it as fact, including InfoWars and, later, Fox News. It is a classic example of the cascading citations effect; the repetition of the conspiracy theory by official news sources took the rumor from the wilderness of Reddit and 4chan message boards to the desk of the president.

Integration

Integration is the point at which purposefully misleading information becomes adopted by trusted news sources or is widely disseminated by real users on social media platforms. For peddlers of disinformation, success translates to influence, and widespread political and social influence happens at the point when disinformation is woven into the public discourse. In the money laundering context, integration is the movement of laundered funds into legitimate accounts or businesses. Success for money laundering operations takes many different forms. For some criminal groups, it may amount to the purchase of arms or drugs; for others, investments that will pay dividends into a traditional brokerage account; and for others still, the purchase of expensive goods. By the time funds are this advanced within a money laundering scheme, it is typically beyond the ability of financial institutions to confidently link them to a crime or otherwise suspicious activity. Governments themselves can struggle. For example, the Treasury Department's financial intelligence unit maintains an administrative authority to declare that a product class, bank, or country is of money laundering "concern." The action need not prove money laundering, only that there is a "concern," or reasonable grounds for strong suspicion. According to evaluations released by the global standard setting body Financial Action Task Force, most governments outside the United States, Europe, and some Latin American countries struggle to convict any money launderers, and few illicit funds are ever seized.

Similar to actual money laundering, successfully integrated disinformation is hard to identify. Was a voter influenced because they read an ad purchased by the Russian government on Facebook? Did the re-tweeting of an article in a fly-by-night "news website" by thousands of bots lead someone to send the article to family and friends, hence giving the story more credibility? Proving the impact of disinformation is an enormous undertaking. What is known, however, is that once a misleading rumor enters the "mainstream," it is almost impossible to combat, even if it is subsequently debunked. Propagandists thus need only to puncture the porous layer between questionable and credible news sites to achieve their objective — whether the news itself holds up to closer scrutiny is almost irrelevant.

Adapting Policy

The disinformation campaign orchestrated by Russia during the 2016 presidential election was not an isolated case. Similar attempts to launder disinformation for political purposes through bots, middlemen, and "legitimate" third parties occurred before then and continue to this day.

9 Donara Barojan, "The Seth Rich Story in the Kremlin Media," The Atlantic Council's Digital Forensic Research Lab, May 24, 2017.

Much like terrorist financing and money laundering by criminal entities changed the relationship between the government and financial institutions related to combating financial crimes, the willingness of Russia to influence political happenings in the United States and Europe should change what role telecommunications, technology, and social media companies play related to the spread of disinformation. The sophisticated monitoring technologies, information sharing methods, and other processes that have enabled banks to protect their customers, root-out potential criminals, and provide meaningful information to the government on unusual activity can and should be employed by technology and social media companies to combat the malign influence of state-sponsored influence campaigns. Several approaches used by financial institutions to combat illicit financial activity can be adopted by social media and technology companies to combat information laundering:

Understand the Source of Funds

Financial institutions go to great lengths to understand the "source of wealth" of direct customers. This includes anything from understanding what job a customer holds and how an account is initially funded to the type of company sending money through the bank. For social media companies, information about the origin of funds can provide greater clarity into the objective of paid advertisement or new accounts. For example, the purchase of an advertisement with foreign currencies, through limited liability companies located in low transparency jurisdictions, or from an organization with ties to groups known to spread disinformation may hint at a secondary motive.

Set up Warning Signs. Technology systems that compare incoming and outgoing financial activity against pre-determined scenarios about known money laundering techniques help banks identify potentially illicit activity. Social media and technology companies should develop similar rules to root-out the spread of disinformation. The rapid set-up of dozens or hundreds of accounts through common IP addresses, posts outside of normal daytime hours for an account's claimed physical location, and routinely retweeting or sharing posts from other accounts with no additional activity, among other suspicious activity, should lead social media and technology companies to evaluate the true purpose of those accounts. Banks update the pre-determined scenarios within their technology systems on a routine basis as they receive information about how illicit actors adapt their behavior. Similarly, social media and technology companies need to account for these changes and routinely consider new "warning signs" when identifying actors seeking to spread disinformation.

Share Information

A legal authority established under the USA PATRIOT Act is used by financial institutions to formally share select information on money laundering, sanctions evasions, and terrorist financing in order for the U.S. government to provide information on those risks to banks. Routine and robust sharing of specific information about disinformation campaigns (including which accounts were set up, identified techniques to evade controls, trends, and payment methods) between social media and technology companies would better equip all to combat its spread. However, sharing this type of information has been sporadic due to the fact that the monetization of user data is central to the business models of tech companies.

Keep an Open Mind About Disinformation

Certain money laundering techniques for many decades have served as an effective method for bad actors to move funds. However, other techniques are wholly new and are often a response to increased law enforcement attention. The spread of disinformation through social media and technology companies has not halted since the 2016 U.S. presidential election and is almost certain to be used in the future by the Russian government and other state and non-state actors. Some of the techniques for spreading disinformation will remain the same, while others will certainly evolve with the emergence of new technologies. Much like banks are less adept at identifying illicit activity when they assume bad actors do not change their methods for moving money, social media and technology companies that do not account for future changes will fail to combat disinformation.

The views expressed in GMF publications and commentary are the views of the author alone.

About the Authors

Kirill Meleshevich previously analyzed global money laundering and sanctions risks for the U.S. Treasury Department.

Bret Schafer is the coordinator of communications, social media, and digital content at the Alliance for Securing Democracy.

About the Alliance for Securing Democracy

The Alliance for Securing Democracy is a bipartisan, transatlantic initiative housed at The German Marshall Fund of the United States (GMF) that is committed to developing comprehensive strategies to defend against, deter, and raise the costs on Russian and other state actors' efforts to undermine democracy and democratic institutions. The Alliance is informed by a bipartisan, transatlantic advisory council composed of former senior officials with experience in politics, foreign policy, intelligence, Russia, and Europe — bringing deep expertise across a range of issues and political perspectives.

About GMF

The German Marshall Fund of the United States (GMF) strengthens transatlantic cooperation on regional, national, and global challenges and opportunities in the spirit of the Marshall Plan. GMF does this by supporting individuals and institutions working in the transatlantic sphere, by convening leaders and members of the policy and business communities, by contributing research and analysis on transatlantic topics, and by providing exchange opportunities to foster renewed commitment to the transatlantic relationship. In addition, GMF supports a number of initiatives to strengthen democracies. Founded in 1972 as a non-partisan, nonprofit organization through a gift from Germany as a permanent memorial to Marshall Plan assistance, GMF maintains a strong presence on both sides of the Atlantic. In addition to its headquarters in Washington, DC, GMF has offices in Berlin, Paris, Brussels, Belgrade, Ankara, Bucharest, and Warsaw. GMF also has smaller representations in Bratislava, Turin, and Stockholm.

1700 18th Street NW
Washington, DC 20009
T 1 202 683 2650 | F 1 202 265 1662 | E info@gmfus.org
http://www.securingdemocracy.org/