The Secret War of Cyber Influence Operations and How to Identify Them

David Tayouri

Social media is an effective way of influencing human society and behavior and shaping public opinion. Cyber influence operation means using cyber tools and methods in order to manipulate public opinion. Today, many countries use cyberspace, and specifically social media, to manage cyber influence operations as part of holistic information warfare. Most of these operations are done covertly and, therefore, identifying them is challenging; moreover, it is not an easy task to differentiate between legitimate or malicious influence operations. This paper will describe cyber influence operations, the potential damages that they could incur, and how they are conducted. Furthermore, the paper will analyze the challenges of identifying such operations and will detail several indicative parameters with which cyber influence operations can be identified.

Keywords: Cyber influence, influence operation, social media, social engineering, cyberwarfare

Introduction

The digital era has changed the way we communicate. Nowadays, relationships and conversations between people take place through the web and digital communication. Using social media—such as Facebook and Instagram—and social applications—such as WhatsApp and Telegram—we can keep in touch with our friends and family; share posts, messages, pictures, and

David Tayouri is deputy director of Engineering, the National and Aviation Cyber Programs Directorate, Cyber Division, ELTA Systems Ltd. at the Israel Aerospace Industries (IAI). The author would like to thank Mr. Aaron (Ronnie) Eilat and Mr. Mark Ellins for reviewing this article and for their thoughtful comments.

videos; share our experiences with each other, be updated on our friends' statuses, and read their posts.

Social media, which is vastly used by many people around the world, is also an effective way of influencing human society and behavior and shaping public opinion. By sharing a post, tweeting an opinion, contributing a discussion in a forum, and sharing a sentimental or political picture, we can influence others and sometimes convince them with our opinion. Now imagine that you could participate in hundreds and thousands of digital conversations—you would have the chance of influencing large communities.

Using cyber tools and methods to manipulate public opinion is called a cyber influence operation. These operations may have different purposes: influencing psychologically, hurting morale, influencing public awareness, instilling a lack of control and the inability to protect the normative way of life, and more. Since these operations may cause (psychological) damage, they are also known as disinformation cyberattacks.

Today, many countries use cyberspace, and specifically social media, to manage cyber influence operations as part of holistic information warfare. Most of these operations are done covertly; in cases where the operation is revealed, it would be difficult to prove who stands behind them. Influence operations can be aimed at the general public with generic statements or can be directed at a specific audience with targeted messages in order to achieve more effective influence and to control their responses. An example of a response could be voting for a specific candidate or party in an election as was witnessed during the US presidential elections in 2016.

Identifying cyber influence operations is challenging. It is not an easy task to identify influence and specifically to differentiate between legitimate and malicious influence operations. Promoting a product or a decent idea is legitimate, even as an influence operation. Incitement, promotion of radical or violent acts, and intervention in democratic elections are examples in which malicious influence operations could be used. Nevertheless, it is important for governments, through defense organizations and law enforcement agencies, to identify malicious influence operations, in order to prevent them or, at least, to reduce their damages. Today, there is no systematic way of identifying cyber influence operations and differentiating between legitimate and malicious influence operations.

The following sections describe cyber influence operations and their potential damages, how cyber influence operations are conducted, and which tactics they use. The challenges of identifying cyber influence operations are analyzed and several indicative parameters with which cyber influence operations can be identified are detailed. The final section presents a case study of a cyber influence operation.

Cyber Influence Operations

A cyber influence operation can be defined as focused efforts to understand and engage key audiences in order to create, strengthen, or preserve conditions favorable for advancing interests, policies, and objectives, through the use of coordinated programs, plans, themes, messages, and products.[1] To put it simply, cyber influence operations create communications and interactions with the aim of influencing target audiences in order to change their opinion and/or behavior. If the purpose is controlling the responses of the group members, this is called *perception management*.

A theory similar to perception management, studied mainly in Russia, is *reflexive control*.[2] Reflexive control is defined as a means of conveying to a partner or an opponent specially prepared information to incline him/her to voluntarily make the predetermined decision desired by the initiator of the action. A "reflex" involves the specific process of imitating the opponent's reasoning or the opponent's possible behavior, thereby causing one to make an unfavorable decision. In order to influence a state's information resources, reflexive control measures can be used against its decision-making processes. This aim is best accomplished by formulating certain information or disinformation designed to affect a specific information resource. If successfully achieved, reflexive control over the opponent makes it possible to influence their plans, their view of the situation, and how they would fight. In other words, one side can impose its will on the other and cause them to make a decision inapposite to a given situation.

A close term to cyber influence in the military context is *influencing maneuver*, which is the process of using (cyber) operations to get inside an enemy's decision cycle or even forcing that decision cycle to direct or

1 Eric V. Larson, and others, *Understanding Commanders' Information Needs for Influence Operations* (Santa Monica: Rand Corporation, 2009).

2 Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* 17, no. 2 (2004): 237–256.

indirect actions. It is a broad form of maneuvering intended to gain and maintain information superiority and dominance and to maintain freedom of maneuver in cyberspace.[3] Influencing maneuver can be used in direct or indirect operations. A direct example of influencing maneuver could include actions such as compromising command and control systems and manipulating data subtly in order to degrade the confidence that a commander has in the systems and to slow down decision cycles. Indirect actions might include feeding compromised and manipulated data to the media in order to force a desirable reaction from an enemy. In this article we will focus on indirect actions.

Influence operations have emerged as a major concern worldwide. They come under different names and in various flavors—fake news, disinformation, political astroturfing, information attacks, and so forth. They may arrive as a component of hybrid warfare—in combination with traditional cyberattacks (use of malware)—and with conventional military action or covert kinetic attacks.[4]

An influence operation may have different purposes and potential effects/damages. In times of peace, the purpose of influence operations can be promoting desired ideas or leading groups to preferred directions. An example is a political party that manages a campaign to convince its constituents to vote for the party. If the same operation is performed by a foreign country, this, of course, will be deemed as intervening in a sovereign country's domestic affairs. Foreign intervention could damage the trust that the citizens have in their government, because they cannot be sure that the same government would be elected without the foreign intervention.

In times of conflict or war, the purpose of influence operations can be to create anti-government discussions, turn public opinion against government actions (e.g., actions of war), hurt public morale (e.g., creating a feeling of insecurity because of government actions), and so forth, all with the aim of giving a sense that the government has no control or ability to protect the

3 Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," *2012 4th International Conference on Cyber Conflict (CYCON 2012),* (Tallinin: NATO CCD COE Publications, 2012), https://www.ccdcoe.org/publications/2012proceedings/3_3_Applegate_ThePrincipleOfManeuverInCyberOperations.pdf.

4 "Army Researchers Join International Team to Understand, Defeat 'Disinformation' Cyberattacks," *ARL Public Affairs*, December 5, 2017, https://www.army.mil/article/197316/army_researchers_join_international_team_to_understand_defeat_disinformation_cyberattacks.

normative way of life, which eventually may weaken the country's army in the battlefield.

Influence operations can be aimed at the general public or at a specific audience, which can be targeted using online databases or social networks. Influence operations aimed at the general public will include generic statements, which will have a minimal influence at the micro level on individuals but can still reach the desired effect at the macro level. Influence operations aimed at specific audiences will use statements tailored to that audience in order to be more effective.

How Cyber Influence Operations Are Conducted

The first step in conducting an effective cyber influence operation is defining the goal of either building one—by promoting a subject, strengthening it, improving public opinion of it—or harming one by attacking the opponents, weakening the adversaries, and creating negative public opinion. The second step is determining the coverage and audience: a wide audience, targeted groups, or a small group of influencers; radical or consensus groups; and which gender, age, race, religion, and so forth will best serve the goal. The third step is selecting the social networks and forums in which the influence operation will be conducted and determining the interaction between the selected medium and other intermediaries. The fourth step is determining the tools for spreading the messages: fake profiles, bots, or trolls. Fake profiles may have a better reputation, but they need manual intervention. Bots can be programmed to reply automatically to defined content, but they may be easily identified as bots. Trolls are used when using aggressive negative content, usually when the goal is to attack opponents. The last step is defining the appropriate messages and publishing them intensively, according to the defined goal and audience. Figure 1 below depicts the steps of operating cyber influence operations.

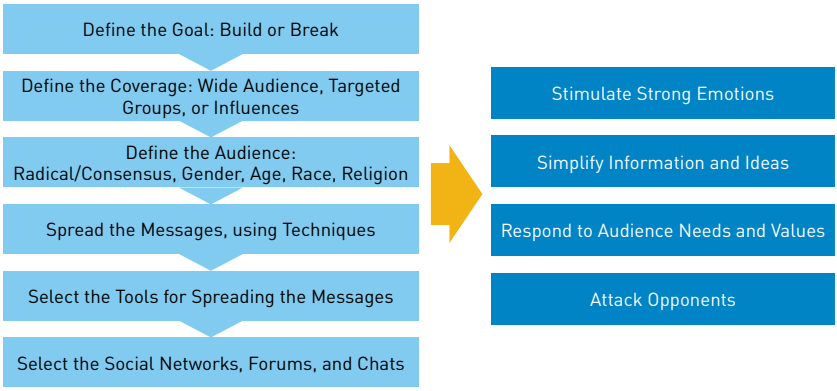

Figure 1. The Steps of Operating Cyber Influence Operations

Propaganda has always been a common way of influencing people. Modern propaganda is very effective since it relies on the digital and social media. It can easily reach many people or selected groups and uses a large number of posts to achieve its goal. Cyber influence operations may use the same techniques as propaganda to successfully influence people,[5] including:

- **Stimulating strong emotions** such as fear, hope, anger, frustration, and sympathy in order to direct audiences toward the desired goal. In the deepest sense, it is a mind game—the skillful influence operator exploits people's fears and prejudices. Successful influence operators understand how to psychologically tailor messages to people's emotions in order to create a sense of excitement and arousal for the purpose of suppressing critical thinking and exasperating emotions instead.
- **Simplifying information and ideas** by using accurate and truthful information, half-truths, opinions, lies, and falsehoods. A successful influence operation tells simple stories that are familiar and trusted, often using metaphors, imagery, and repetition to make them seem natural or "true." Oversimplification is effective when catchy and memorable short phrases become a substitute for critical thinking. Oversimplifying information does not contribute to knowledge or understanding; rather because people naturally seek to reduce complexity, this technique of influence operation can be effective.

5 "Recognizing Propaganda," *Mind Over Media*, https://propaganda.mediaeducationlab.com/techniques.

- **Responding to audience needs and values** by conveying messages, themes, and language that appeal directly—and many times exclusively—to specific and distinct groups within a population. A cyber influence operator may appeal to people using their racial or ethnic identities, hobbies, favorite celebrities, beliefs and values, or even personal aspirations and hopes for the future. Using different social media profiles, this task becomes easier and more effective, since each profile can be adjusted to the target audience in order to achieve the best influence result.

  Sometimes, universal deepest human values—the need to love and be loved, to feel a sense of belonging and a sense of place—are activated. By creating messages that appeal directly to the needs, hopes, and fears of specific groups, an influence operation becomes personal and relevant. When messages are personally relevant, people pay attention and absorb key information and ideas.
- **Attacking opponents** by serving as a form of political and social warfare to identify and vilify opponents. It can call into question the legitimacy, credibility, accuracy, and even the character of one's opponents and their ideas. Because people are naturally attracted to conflict, an influence operation can make strategic use of controversy to get attention. Attacking opponents also encourages "either-or" or "us-them" thinking, which suppresses the consideration of more complex information and ideas. Furthermore, influence operations can also be used to discredit individuals, destroy their reputation, exclude specific groups of people, incite hatred, or cultivate indifference.

Challenges of Identifying Cyber Influence Operations

In order to identify cyber influence operations, first we should identify cyber or social influence. Therefore, one of the basic challenges is to define what social influence is and how to measure it within a network. Social influence is defined as "consciously or subconsciously persuading others from your thoughts, beliefs or actions."[6] There are three categories in defining social influence: **actors**, **interactions**, and **networks**.

To achieve the largest possible audience, in many cases, cyber operators approach influencers. There are different indicators for identifying the potential

6 D.M. Kahan, "Social Influence, Social Meaning and Deterrence," *Virginia Law Review* 83, no. 2 (1997): 349–395.

of an **influential actor** (i.e., influencer): active minds, trendsetters, social presence and impact, social activity, charisma, expertise, authority, number of followers/friends, and more. An actor has influence in a network if the message is shared outside his/her own network; the message is shared by others in the network; the actor has a large number of contacts; the actors causes others to read a message; and the speed in which a message is shared/used within a network is high.

The **influential interaction** can be measured with different indicators. Dutch researchers have found that the influence of an interaction largely depends upon the following: the number of times a message has been shared; the types of reactions that a message causes; the number of times a message has been quoted; number of readers/listeners reached; and if the message brings a large group of unique visitors.[7]

One of the commonly used and influential sites for interaction in cyberspace are weblogs. The following is different criteria for testing influence within the context of weblogs:[8]

- Network centrality score—measures the reputation of an individual. Is he/she a central person in a network or just someone with a limited number of contacts?
- Hyperlink authority score—measures the number of links to a blog as a criterion for influence.
- Site traffic score—measures the number of website visitors.
- Community activity score—relates to the number of comments that a blog evokes.

Similarly, additional studies have associated other indicators with **influential social networks**, including the social distance between two actors, reciprocity, multiplexity, size of the network, density, connectivity, centrality, emotional value, group cohesion, and clustering.

7 Wouter Vollenbroek, Sjoerd de Vries, Efthymios Constantinides, and Piet Kommers, "Identification of Influence in Social Media Communities," *International Journal of Web Based Communities* 10, no. 3 (2014): 280–297.

8 Dave Karpf, "Measuring Influence in the Political Blogosphere: Who's Winning and How Can We Tell?" *Politics and Technology Review* (2008): 33–41, http://www.the4dgroup.com/BAI/articles/PoliTechArticle.pdf.

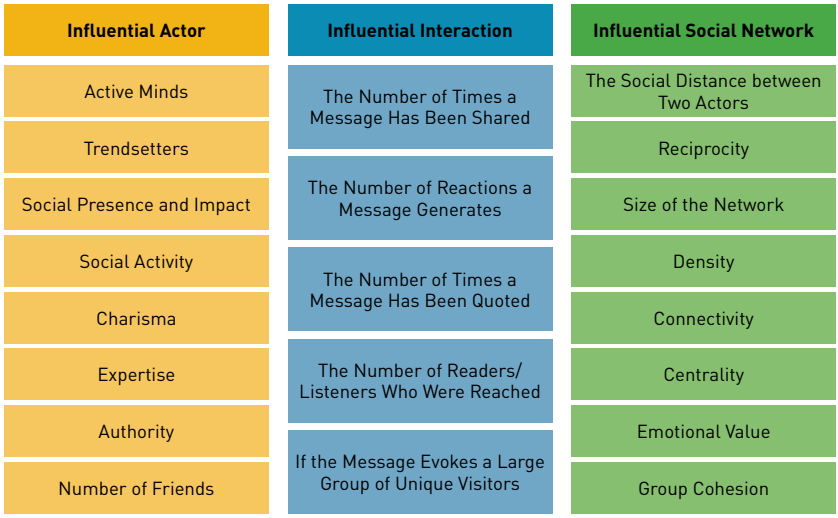

Figure 2. Social Influence Indicators

These well-defined indicators can be used to find influential actors, interactions, and networks, which, in turn, can help us to better identify social influence. Figure 2 above summarizes the social influence indicators.

After identifying social influence, the next challenge is differentiating between legitimate and malicious influence operations. Sometimes the legitimacy of an influence operation is in the eyes of the beholder. Most people will agree that incitement and promotion of radical or violent acts constitute malicious influence operations, and that promoting a decent idea is usually legitimate freedom of speech. But what about political ideas or statements that are expressed against a country's leadership? Well, it may depend on the country's values and regime. Let's take a democratic regime, in which a person can criticize anything and anyone, including the country's leader. If this was done by an army of bots, which were programmed to automatically spread statements against the leading party, the legitimacy of the statements would not be very clear, especially when using bots is prohibited by most countries. If this army was managed by a foreign actor, it would probably be considered as foreign intervention in a sovereign's democracy.

Sometimes, to influence effectively, fake news is used. For instance, Saudi Arabia and the UAE worked to sway American public opinion and other Arab countries against Qatar through online and social media campaigns, by accusing Qatar of supporting terrorism and destabilizing the region, a

charge Doha rejected, and which eventually appeared to be false. The result of this campaign was that during June 2017, Saudi Arabia and the UAE led other Arab countries to cut diplomatic relations with Qatar.[9] We can agree that using fake news is not legitimate and may indicate a malicious influence operation, but the real challenge is in identifying it. Mostly, fake news is published together with other authentic news, making it difficult to spot. Identifying fake pictures is also challenging, with all the advanced picture editing tools available today. The situation becomes complicated when a particular post may include some facts, some bogus facts, and some commentary that naturally is subjective, depending on the writer's values and beliefs. In social media, such a post receives comments from others, reflecting their opinions and perspectives, which make it even harder to identify the false elements.

Another challenge in identifying cyber influence operations is that the process should be done in near real time. In social media, news spreads very fast; therefore sometimes until a fact is revealed as false, the damage has already been done and influence operation goals have been promoted. For example, spreading fake or semi-fake news about a candidate a few days before the elections may change the results.

After a cyber influence operation is identified, we usually want to know who stands behind it and collect evidence to prove it. The challenge here is that the people or the group behind the influence operations usually hide their tracks and do not reveal their true identity, by using bots and fake profiles in social media, and by concealing their communication parameters (such as their IP) with the use of dedicated browsers for anonymous browsing or by using proxy servers.

Indicative Parameters for Identifying Cyber Influence Operations

To identify cyber influence operations, the published content—text, pictures, and videos—in the various social networks should be monitored and analyzed using operations research and advanced algorithms, taking into account many

9 Josh Wood, "How a Diplomatic Crisis among Gulf Nations Led to a Fake News Campaign in the United States," *PRI*, July 24, 2018, https://www.pri.org/stories/2018-07-24/how-diplomatic-crisis-among-gulf-nations-led-fake-news-campaign-united-states.

content- and communication-oriented parameters. The following indicative parameters may help identify a cyber influence operation:

- **Use of avatars, bots, and trolls**—a good influence operation will hide its operators in order to achieve the most effective results. There are several ways of anonymizing the influence operation, but two of the most used tools are avatars and bots. Avatars are virtual identities in social media, which hide their operator's true identity. Bots are small agents, which are programmed to automatically respond to specific posts or publish automatic posts to promote their programmed idea/product. Many tactics can be used to identify bots. Two researchers have found a number of traits to spot a bot, such as having a sleepless account, engaging in high-volume retweeting, replying to content that contains certain keywords, using stolen profile images, having unreal profile names, showing significant gaps in the account activity, and more.[10]
- **Publishing of posts and news by factors outside of the country**—it is a legitimate action when people try to convince other people and promote their own ideas or beliefs, as long as this is done in their own country or done from another country but without hiding their identity. But if someone from another country impersonates a local citizen, it is suspicious and should be investigated. A good example of this is trying to influence results of elections in another country. It should be mentioned that it is not an easy task to discover the real source of published content. VPS (Virtual Private Server) based in the target country may be used to mask the location of the individuals involved. Email accounts based in the target country and linked to fake or stolen identities may be used to back the online identities. These identities may also be used to launder payments through PayPal and cryptocurrency accounts.
- **Publishing of fake news**—this is one of the more efficient methods of influencing public opinion as witnessed in the case of the US and French elections. Researchers from Stanford found that 62 percent of American adults get their news on social media, that the most popular fake news stories were widely shared on Facebook, and that many people exposed

10 Bill Fitzgerald and Kris Shaffer, "Spot a Bot: Identifying Automation and Disinformation on Social Media," *Data for Democracy*, June 5, 2017, https://medium.com/data-for-democracy/spot-a-bot-identifying-automation-and-disinformation-on-social-media-2966ad93a203.

to fake news stories report that they believe them.[11] This means that fake news disseminated on social media is a good tactic for influence operations and, therefore, a good indicator for identifying this kind of operation.

- **Publishing a large number of items on a specific subject**—to reach as many people as possible and in order to increase the influence, numerous items about the subject of influence need to be published. For instance, if one country plans a military action against another country, the latter could publish a large number of posts and tweets against the action, addressing the possible damages to the economy, exaggerating the number of casualties, the harm to human rights, and so on.
- **A sudden change of public opinion**—when looking at specific groups on social media and internet forums, changes in public opinion over a short period of time may indicate foreign intervention, because changes in opinions tend to be gradual. For example, in an election, if a leading candidate suddenly loses the lead in a day or two, this could be an indication of external intervention.
- **Publishing radically negative phrases**—to achieve a fast and effective change of public opinion in relevant groups or forums, extremely negative phrases may be used and may indicate an incitement operation. For instance, if a political group is vilified by calling into question their legitimacy and credibility by using extremely negative expressions, this should raise a red flag.

Figure 3 below depicts the indicative parameters for identifying cyber influence operations. A single parameter is not enough to indicate an influence operation, but a combination of several parameters could suggest that an influence operation is being conducted. In addition, the process can be automated by an algorithm that will combine all the indicators, although they may differ depending on the situation. The indicative parameters should be given different weight according to their context.

11 Hunt Allcott and Matthew Gentzkow, "Social Media and Fake News in the 2016 Election," *Journal of Economic Perspectives* 31, no. 2 (Spring 2017): 211–236, https://web.stanford.edu/~gentzkow/research/fakenews.pdf.

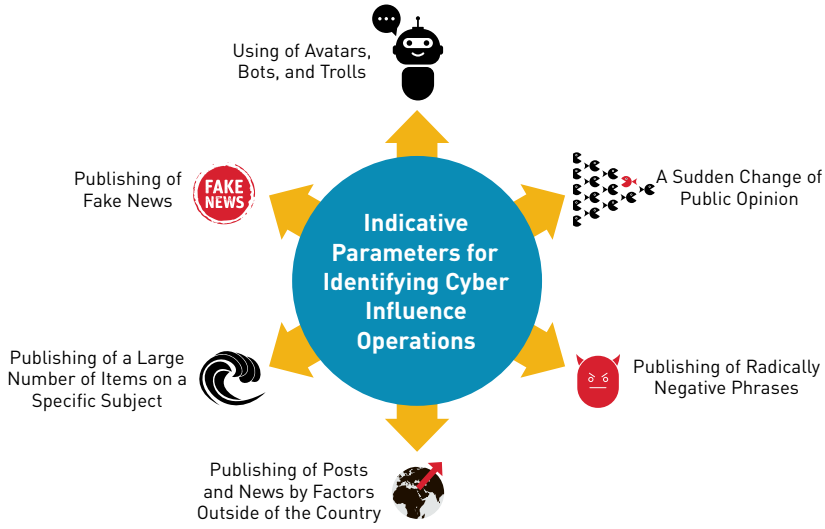

Figure 3. Indicative Parameters for Identifying Cyber Influence Operations

Case Study: Russian Intervention in the US Elections in 2016

Many cases of cyber influence operations were published over the last years, but one of the best known cases is the Russian intervention in the US elections in 2016. Analysis of this case shows that almost all the parameters mentioned in the previous section could be relevant for identifying the Russian influence operation in the 2016 US election:

- Russians publishing posts—On October 7, 2016, the Office of the Director of National Intelligence (ODNI) and the Department of Homeland Security (DHS) jointly stated that the US intelligence community was confident that the Russian government directed the hacking of emails in order to interfere with the US election process.[12] Two reports prepared for the Senate Intelligence Committee by independent researchers reveal that

12 "Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security," *Department of Homeland Security*, October 7, 2016, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

Moscow's intelligence officials reached millions of social media users between 2013 and 2017.[13]

- Use of avatars and trolls—According to a ODNI report, the Russian campaign was multifaceted, including state-funded media, overt propaganda, and paid social media users or trolls.[14] Reports show the trolls used multiple websites to disseminate their narratives.[15] Facebook officials said that 470 fake accounts had been created since June 2015 and were used during the 2016 US election campaign by the Russian company Internet Research Agency (IRA), which is known for using "troll" accounts to post on social media and comment on news websites.[16]
- Fake news—In January 2017, the director of US National Intelligence testified that Russia also interfered in the elections by disseminating fake news promoted on social media.[17] In nearly 110 Facebook posts, including fake images of election machine error messages or ballots, the IRA targeted conservative users with false information about supposed widespread voter fraud aimed at helping Clinton win.[18]

13 Alex Ward, "4 Main Takeaways from New Reports on Russia's 2016 Election Interference," *Vox*, December 17, 2018, https://www.vox.com/world/2018/12/17/18144523/russia-senate-report-african-american-ira-clinton-instagram.

14 "Assessing Russian Activities and Intentions in Recent US Elections," *Office of the Director of National Intelligence*, January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

15 "Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security," *Department of Homeland Security*, October 7, 2016, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

16 Scott Shane and Vindu Goel, "Fake Russian Facebook Accounts Bought $100,000 in Political Ads," *New York Times*, September 6, 2017, https://www.nytimes.com/2017/09/06/technology/facebook-russian-political-ads.html.

17 Ellen Nakashima, Karoun Demirjian, and Philip Rucker, "Top US Intelligence Official: Russia Meddled in Election by Hacking, Spreading of Propaganda," *Washington Post,* January 5, 2017, https://www.washingtonpost.com/world/national-security/top-us-cyber-officials-russia-poses-a-major-threat-to-the-countrys-infrastructure-and-networks/2017/01/05/36a60b42-d34c-11e6-9cb0-54ab630851e8_story.html.

18 "Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security," *Department of Homeland Security*, October 7, 2016, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

- Publishing many items on the candidates—One of the fake news items about Secretary Clinton was shared 800,000 times.[19] Instagram saw an estimated 20 million users engage roughly 187 million times with IRA content related to the election, while Facebook had 76.5 million engagements that reached about 126 million people.[20]
- Many negative phrases about the candidates—According to the ODNI, Russia helped Trump's election chances by discrediting Secretary Clinton and publicly contrasting her as unfavorable.[21] When it appeared to Moscow that Secretary Clinton was likely to win the presidency, the Russian influence campaign focused more on undercutting Secretary Clinton's legitimacy and crippling her presidency from its start, including to impugn the fairness of the election. According to the Computational Propaganda Research Project, the Russian company IRA used many tactics to shape public opinion in the United States by spreading misinformation on social media platforms, exploiting social media platforms for foreign influence operations, and amplifying hate speech or harmful content through fake accounts or political bots.[22]

Other Case Studies

As mentioned above, the 2016 US election was neither the first nor the last known cyber influence operation. Following are a few other cyber influence operations:

- Pro-Russian hackers launched a series of cyberattacks over several days to disrupt the Ukrainian presidential election in May 2014 by releasing

19 Ellen Nakashima, Karoun Demirjian, and Philip Rucker, "Top US Intelligence Official: Russia Meddled in Election by Hacking, Spreading of Propaganda," *Washington Post,* January 5, 2017, https://www.washingtonpost.com/world/national-security/top-us-cyber-officials-russia-poses-a-major-threat-to-the-countrys-infrastructure-and-networks/2017/01/05/36a60b42-d34c-11e6-9cb0-54ab630851e8_story.html.

20 Alex Ward, "4 Main Takeaways from New Reports on Russia's 2016 Election Interference," *Vox*, December 17, 2018, https://www.vox.com/world/2018/12/17/18144523/russia-senate-report-african-american-ira-clinton-instagram.

21 Alex Ward, "4 Main Takeaways from New Reports on Russia's 2016 Election Interference," *Vox*, December 17, 2018, https://www.vox.com/world/2018/12/17/18144523/russia-senate-report-african-american-ira-clinton-instagram.

22 Philip N. Howard, Bharath Ganesh, and Dimitra Liotsiou, "The IRA, Social Media and Political Polarization in the United States, 2012–2018," Computational Propaganda Research Project, 2018, https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf.

hacked emails, attempting to alter vote tallies, and delaying the final result with distributed denial-of-service (DDOS) attacks.[23]

- In December 2016, Ben Bradshaw, a member of the British Parliament, claimed that Russia had interfered in the Brexit (the exiting of the United Kingdom from the European Union) referendum campaign.[24]
- During the 2017 presidential election in France, automated accounts shared fake news about the election, and much of it came from sources that were exposed to Russian influence.[25] Russian influence was introduced into the French political discourse via content about international issues. This content was framed to undermine traditional media sources, minimize issues raised in opposition to Russian activities, or otherwise shift the focus and blame to other actors. The content served to mitigate criticism of Russia and create support for its political positions and, implicitly, the presidential candidates who espouse them.

Cyber influence operations may infect also the commercial space. Nike came under digital attack—a coordinated, operational campaign—after it rolled out the Colin Kaepernick campaign during September 2018.[26] Goals of this cyberattack included driving down the company's sales and share price. The following indicative parameters could be used to identity this operation:

- Use of avatars and bots—Certain groups were promoting a boycott against Nike by organizing echo chambers to mobilize tweets or deploying computer-generating traffic with bots. Inspection of the active users revealed that 426 out of 668 sampled users attacking Nike were avatars.
- Publishing many items against Nike—One of the coordinated influence campaigns had 300 users and generated about 2,133 tweets and retweets in a short time.

---

23 Mark Clayton, "Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers," *Christian Science Monitor*, June 17, 2014, https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers.

24 Joe Watts, "Labour MP Claims It's Highly Probable' Russia Interfered with Brexit Referendum," *Independent*, December 13, 2016, https://www.independent.co.uk/news/uk/politics/russian-interference-brexit-highly-probable-referendum-hacking-putin-a7472706.html.

25 Pierre Haski, "Patterns of Disinformation in the 2017 French Presidential Election," *Bakamo*, 2017, https://www.bakamosocial.com/frenchelection/.

26 Jay Solomon and Aftan Snyder, "Lessons for Brands from the Anti-Nike-Kaepernick Social Effort," *PRNEWS*, February 22, 2019, https://www.prnewsonline.com/social+media-Nike-Kaepernick-APCO-bots-Twitter.

- Using many negative phrases—Users posted at least ten negative tweets or retweets during the campaign.
- A sudden change of public opinion—Nike's share price fell 3.2 percent the day after the campaign debuted.

Conclusion

Social media, which is vastly used by people around the world, is also an effective way of influencing social behavior and shaping public opinion. Cyber influence operation uses cyber tools and methods to manipulate public opinion. Today, many countries use cyberspace, particularly social media, to manage cyber influence operations as part of mostly covert holistic information warfare. When an influence operation is used to intervene in the internal affairs of another country, this may damage the trust that citizens have in their government. In addition, it may cause anti-government discussions, actions, protests, and harm public morale. Therefore, it is important for governments and defense organizations to identify cyber influence operations in order to prevent them or, at least, to reduce their negative influence. Although it is clear how cyber influence operations are conducted and which tactics they use, identifying them is not an easy task, since the influence operators use different masking tactics.

This paper introduced several indicative parameters for identifying cyber influence operations via published content, such as social media. Finding the parameters discussed here is challenging on its own, and each of them individually is not enough evidence of an influence campaign. Nevertheless, they may serve as a good starting point for a situation analysis, and their combined use simultaneously may provide a good indication that an influence operation is being conducted. The case study of the Russian influence operation in the 2016 US elections was a perfect example in which almost all the indicative parameters could be used to identify the operation, even at its earliest stages. This shows that the mentioned indicative parameters can be used systematically for detecting the next cyber influence operation. By constantly monitoring the relevant media, the mentioned practical approach enables early detection of the next cyber influence operation, even by non-expert analysts.

The cyber situation at the national level includes the state's critical national infrastructures, defense and government organizations, and so

forth. This cyber situation includes direct cyber events, including attempts of cyberattack, actual cyberattacks, and damage, but it should include also indirect cyber actions, such as cyber influence operations conducted by other countries. These operations should be considered covert wars and should be handled respectively, including allocating resources to identify and thwart them. Recommended further work includes determining additional indicative parameters, automating the influence operation identification process, and suggesting ways to defend against these operations.