BIPSS Commentary
www.bipss.org.bd March-2021
BIPSS Towards a Secure World

Influence Operations

A short commentary by *Simen Agnalt Nilsen

The latter part of the 2010´s saw the introduction of expressions such as "post-truth" and "fake news". In fact, these terms became so influential that they were officially declared international word of the year[1] in 2016,[2] and 2017,[3] respectively. In addition, "influencer" was short-listed for word of the year in 2019.[4] Combined, this paints a picture of a modern public sphere defined by ambiguity and the difficulty of distinguishing right from wrong. A prominent, but perhaps less conspicuous feature is the phenomenon of anonymous actors seeking to influence the behaviour of others through the spread of competing narratives, misinformation and disinformation. What has become known as "Influence Operations" is gaining attention both by practitioners and researchers of security in recent years.

This commentary seeks to shed some much-needed light on what influence operations are by placing it into a historical context and empirically illustrating its use trough the now quite famous case of the Russian interference in the 2016 United States (US) elections. Understanding what influence operations are and how they operate, it will also inquire into the methods of defence against influence operations.

The phenomenon of influence operations

Influence operations may be understood as coordinated and systematic efforts by an initiating actor directed towards an audience with the motivation of gaining a competitive advantage.[5] [6]

---

* *Simen is an Erasmus scholar at the University of Glasgow. He is currently working as a Research Intern at BIPSS.*

[1] International word of the year in the English language.

[2] BBC, "'Post-Truth' Declared Word of the Year by Oxford Dictionaries," BBC News, November 16, 2016, sec. UK, https://www.bbc.com/news/uk-37995600#:~:text=Oxford%20Dictionaries%20has%20declared%20%22post.

[3] Alison Flood, "Fake News Is 'Very Real' Word of the Year for 2017," the Guardian (The Guardian, November 2, 2017), https://www.theguardian.com/books/2017/nov/02/fake-news-is-very-real-word-of-the-year-for-2017.

[4] Collins Dictionary, "Collins Word of the Year 2019 Shortlist - Collins Dictionary Language Blog," Collins Dictionary Language Blog, November 7, 2019, https://blog.collinsdictionary.com/language-lovers/collins-word-of-the-year-2019-shortlist/.

[5] Arild Bergh, "Påvirkningsoperasjoner I Sosiale Medier – Oversikt Og Utfordringer" (Forsvarets Forskningsinstitutt (FFI), June 17, 2020).

[6] Eric V. Larson et al., "Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities," Www.rand.org, May 27, 2009, https://www.rand.org/pubs/monographs/MG654.html.

[7] Although influence operations initiated by states have received most attention in recent years, private actors with profit-driven motives are also engaged. Influence operations today are much facilitated by advances in communication and information technology and the easy access to large amounts of people through social media. Social media platforms also play an important role by allowing initiators to easily hide their identity. This is all compounded by cyber-space remaining a space where innovation exceeds legislation. Although malign operations intending to spread fake-news or disinformation receive a disproportionate amount of attention, it is important to note that systematic efforts can also be well-intending. An operation may for instance be initiated on the grounds of disseminating unfiltered information into a space where information is restricted and narratives monopolized.

Influence operations have low barriers of entry, providing fertile grounds for actors seeking to benefit from the vail of ambiguity cyber-space provides. Capable and motivated actors can initiate influence operations at a low cost, all-while keeping their identities and intentions hidden.

Although the phenomenon of influence operations is quite recent, operations intending to influence the behaviour of an adversary without the use of force is not particularly novel. Throughout history the idea of "winning the hearts and minds" of an adversary through psychological methods rather than violence is seen frequently.[8] For instance, Alexander the Great used the manipulation of elites and cultural infiltration throughout his campaigns across Europe and South-Western Asia[9]. The Cold War also became a hot-bed for influence operations. For instance, the Russian intelligence organization (KGB) was engaged with influence operations operating under a doctrine of "weaponized relativism", or RAND´s perhaps catchier "firehose of falsehoods".[10] The firehose of falsehoods intends to describe a procedure which involves the constant generation of numerous narratives leading to the muddying or watering out the truth. If enough challenging interpretations of the truth is disseminated and accepted, the actual truth will be distorted and possibly confused with competing, misleading narratives[11]. The US also sought to infiltrate the Soviet information sphere through the dissemination of ideals of democracy, capitalism and individual freedom through radio outlets such as "Radio Free Europe" in Central-Eastern Europe and "Radio Marti"

---

[7] Bruce Schneier, "8 Ways to Stay ahead of Influence Operations," Foreign Policy, August 12, 2019, https://foreignpolicy.com/2019/08/12/8-ways-to-stay-ahead-of-influence-operations/.
[8] Talal Al-Khatib, "Hearts and Minds: History of Psychological Warfare," Seeker, April 29, 2015, https://www.seeker.com/hearts-and-minds-history-of-psychological-warfare-1769783167.html.
[9] Sunil Narula, "Psychological Operations (PSYOPs): A Conceptual Overview," Strategic Analysis 28, no. 1 (January 2004): 177–92, https://doi.org/10.1080/09700160408450124.
[10] Christopher Paul, "The Russian 'Firehose of Falsehood' Propaganda Model," Rand.org (RAND Corporation, 2016), https://www.rand.org/pubs/perspectives/PE198.html.
[11] Boris Nemtsov, "The Guardian View on Russian Propaganda: The Truth Is out There | Editorial," the Guardian, March 2, 2015, <a href="https://www.theguardian.com/commentisfree/2015/mar/02/guardian-view-russian-propaganda-truth-out-there">

on Cuba. The Russian firehose of falsehood strategy, Radio Free Europe and Radio Marti are all still active today.[12] [13] [14]

Although past operations bear similarities to today´s influence operations, there are important differences. Most notably this includes the significance of social media and other online mediums. Important is also the fact modern actors have greater and more rapid access to a wide public, all-while keeping their identities hidden through a veil of anonymity. Further complicating matters is the fact that state-led operations today often outsource their activities to external entities, thereby obscuring links to the actual initiator. This also allows states to avoid attribution by pushing responsibility onto others.

The difficulty of attribution essentially makes influence operations difficult to both defend and take action against.[15] First of all, those on the receiving end of influence operations will often be hesitant to accuse or counter-act against an incident which they cannot beyond reasonable doubt link an actor. To illustrate, even though country B can prove the involvement of country A in incident C, country B´s ability to retaliate to will be limited. Since influence operations are situated in the "gray zone", meaning they fall below the conventional threshold of war, responsive acts will most often be modest in order to avoid escalating tensions. Practically, states are left with the choice between diplomatic or economic sanctions – both of which can be viewed aggressively – both of which come with deadweight consequences – and none of which can guarantee the alteration the initiators behaviour.

Overall, influence operations offer low-intensity, low-cost, and relatively easily operated undertakings with the potential of high rewards. Behind a veil of anonymity, state actors can employ a plethora of methods intending to either harass or inject polarizing and destabilizing narratives on the receiving end.[16] Such can be well illustrated through the case of the Russian interference of the US presidential elections of 2016.

Russia´s interference in the 2016 elections

The Russian interference in the 2016 US presidential election has become a notorious example in discussions on influence operations. As it became clear in the 2019 "Mueller Report" Russia

---

[12] Ibid.
[13] Lizette Alvarez, "Radio and TV Martí, U.S. Broadcasters to Cuba, Emerge from Cold War Past Facing Uneasy Future (Published 2015)," *The New York Times*, March 24, 2015, sec. U.S., https://www.nytimes.com/2015/03/25/us/radio-tv-marti-cuba.html.
[14] Radio Free Europe RL, "History," RFE/RL (RFE/RL, May 12, 2019), https://pressroom.rferl.org/history.
[15] Elise Thomas, Natalie Thompson Thompson, and Alicia Wanless, "The Challenges of Countering Influence Operations," Carnegie Endowment for International Peace, June 10, 2020, https://carnegieendowment.org/2020/06/10/challenges-of-countering-influence-operations-pub-82031.
[16] Samantha Bradshaw, "Influence Operations and Disinformation on Social Media," Centre for International Governance Innovation, November 23, 2020, https://www.cigionline.org/articles/influence-operations-and-disinformation-social-media.

had interfered in the US elections in a "sweeping and systematic fashion".[17] Russia's objectives were threefold; to undermine the American people's confidence in their electoral system, to amplify existing social divisions and cause mistrust towards president elect and former secretary of state Hillary Clinton.[18] [19] Social media provided Russia with an open and poorly regulated platform with a large, and direct access the American public. Aware of existing divisions in American society, Russia could undermine public discourse through the injection of divisive narratives, amplification of stigmatizing ideas and instillation of hostile opinions. Russia also sought to weaponize identities through the use of hyperbolic narratives with the intent of deteriorating people's ability to rationalize and reflect over the divisive nature of their own views and opinions.[20]

The Russian operation used sophisticated outlets for fake news, also known as "content farms" or "content mills". [21] A content farm is quite simply a content producing entity which is operated by churning out large amounts of low-quality content. In addition to content farms, bots were used to inflate viewer and share counts across social media platforms. All-together this formed quite a robust and believably well-funded-operation. How much of an impact the Russian efforts had in influencing the American public is disputed, albeit, the magnitude of the Russian effort is demonstrated by the fact that an estimated 19% of all tweets related to the election were shared by Russian bots[22].

Today the Russian farms are better known under The Internet Research Agency (IRA). The IRA is still active in setting up fake social media accounts and participating in online discussions with the aim of inciting aggressive and emotional reactions.[23] During the Covid-19 pandemic the IRA has been active in activities seeking to undermine public trust in national strategies and cause distrust to otherwise trusted sources of information concerning the pandemic.[24]

It is not just by Russia that has engaged in influence operations. Other countries such as China, Iran, USA, Saudi Arabia and Turkey along with many other private, profit-motivated

---

[17] Robert Mueller, "Report on the Investigation into Russian Interference in the 2016 Presidential Election" (US Department of Justice, March 2019).
[18] Sophie Marineau, "Fact Check US: What Is the Impact of Russian Interference in the US Presidential Election?," The Conversation, September 29, 2020, <a href="https://theconversation.com/fact-check-us-what-is-the-impact-of-russian-interference-in-the-us-presidential-election-146711"
[19] Arild Bergh, "Social Network Centric Warfare - Understanding Influence Operations in Social Media" (Norwegian Defence Research Establishment (FFI), October 4, 2019).
[20] Dana Weinberg and Jessica Dawson, "From Anti-Vaxxer Moms to Militia Men: Influence Operations, Narrative Weaponization, and the Fracturing of American Identity," 2020, https://doi.org/10.31235/osf.io/87zmk.
[21] The Reporter, "The Content Mill Empire behind Online Disinformation in Taiwan - 報導者 the Reporter," www.twreporter.org, December 26, 2019, https://www.twreporter.org/a/information-warfare-business-disinformation-fake-news-behind-line-groups-english.
[22] Marineau, (2020)
[23] Thomas,Thompson and Wanless, (2020)
[24] Wesley R. Moy and Kacper Gradon, "COVID-19 Effects and Russian Disinformation Campaigns," HOMELAND SECURITY AFFAIRS, December 9, 2020, https://www.hsaj.org/articles/16533.

actors are also actively engaged. With influence operations growing in scope and complexity question may be raised of how to best construct a meaningful defence. The coming section will consider various methods social media companies, states and the broader society can use in defence. Defending against influence operations is inherently difficult, and elimination is probably impossible. Still, there is plenty of room to limit the impacts.

Defending against influence operations

There are primarily three channels in which influence operations can be dealt with: Platform moderating mechanisms by social media companies, state-driven mechanisms, and empowering public resilience. All options offer unique opportunities, yet all come with short-comings and effective defence will likely require a combination of all three.

1. **Social media companies**

Social media platforms such as Facebook, Twitter, Instagram, YouTube, Reddit etc. offer an important first-line of defence against influence operations through the moderation of content on their platforms. Still, track-records remain mixed. Social media companies have primarily seen themselves as platform services and not publishers, and therefore had less of an interest in acknowledging a responsibility to oversee content. As opposed to publishing companies, social media companies generally do not publish the content on their platforms and have often pushed responsibility of posted content onto its users. [25] There is also an obvious economic incentive here, as substantive human moderation would come at a high cost. This has for a long time, in part, led to outright denial by social media companies that malign entities engage in influence operations on their platforms. Facebook CEO Mark Zuckerberg stated for instance shortly after the 2016 US elections that the thought of misinformation and disinformation originating on Facebook influencing the elections was a crazy idea.[26]

Yet, most platforms have guidelines prohibiting violent extremist content and various forms of hate-speech[27] and some progress has been made in recent years. Nevertheless, with the absence of a specific threat, call to violence, or explicit dehumanization, content easily evades moderation.[28] Content produced by content mills can be both highly inflammatory and offensive, but may still often fall outside the detection algorithms for harmful content. Overall, in the present day it is difficult to filter out unwanted content without resorting to an interpretation of platform-guidelines on a case-by-case basis. Algorithms play a role, yet, given the share quantity of content which is shared on social media platforms every-day, much slips through undetected or remains below a stature of direct incitement to violence, or spread of extremist views.

[25] Ibid.
[26] Bergh (2020:20)
[27] Elise Thomas, Natalie Thompson and Alicia Wanless,(2020:22)
[28] Ibid.
[28] Ibid.

2. State driven mechanisms

Given that social media companies have an inconsistent track-record, states are increasingly exploring mechanisms to regulate cyber space. Concerning this, states, thereof particularly democratic ones, face the puzzle of balancing citizen protection with the freedom of speech. This is an issue far to grave to assess with any meaningfulness in this commentary, instead it is recognized that state driven mechanisms also have inherent short-comings. The issues of attribution and extraterritoriality will be used to illustrate these short-comings.[29]

The issue regarding attribution has already been mentioned. Because of the ease of obscuring identities online, it is difficult to attribute blame and hold actors accountable for their actions. The other challenge is that of extraterritoriality. Quite simply, this means that states have limited jurisdiction outside their own borders. In some cases, law can extend to citizens located outside a country's boarders or foreign nationals in the case of a legal violation of another country. Yet, the state´s ability to act upon such violations remain limited. This is because this usually requires extradition, an act which can be both politically difficult and economically costly. Since influence operations often originate outside a country's jurisdiction, violations are rarely acted upon through legal mechanisms.[30] The issue of attribution only further complicates the matter. It is thus important for states to acknowledge mutual commitments both through bi and multilateral arrangements. Important is also the productive dialogue between security and intelligence across country borders. In reality, however, cooperation is curbed by the fact that initiating and receiving states often do often not maintain the strongest relations. Fruitful engagement with social media companies, both by the exchange of information through open dialogue, and the enforcement of domestic law regulating content originating on their platforms, are areas where states likely will find more success. Finally, and perhaps most importantly, states maintain a crucial function in establishing leading narratives within society. It is thus important for state leaders and other officials to engage in informed, evidence-based and inclusive communication in order to avoid losing public trust and prevent the growth of conspiratorial or misleading counter-narratives

3. Social resilience

Finally, the most effective defence against influence operations occurs through the empowerment of critical thinking and support of social resilience. Such can also be thought of as societal mass immunity to false information, misinformation and disinformation. If enough people are able to identify and critically assess questionable information, they are less likely to be influenced personally and also less likely to act as "useful idiots" by further disseminating false information and subscribing to and spreading toxic narratives. It goes without saying, that not everyone is vulnerable to influence campaigns as some will be more easily able to critically

[29] Ibid. (33)
[30] Ibid.

assess information than others. The task is then to identify what makes people resilient and establish frameworks for a more critical engagement with the many narratives shuffled around in cyber-space. As cyber-specialist and author Bruce Schneier suggests, the public must become "reflexively suspicious", pointing to a trained mechanism of suspicion which becomes active when certain content triggers a negative emotional reaction towards other groups of people[31]. This is obviously no easy task, and every member of society will never be immune to campaigns intending to skew or mislead their interpretation. Nevertheless, if enough people are able to both critically reflect over the content they come across and question their own convictions, venomous narratives will less likely take grip.

Conclusion

Influence operations sprung onto the public scene following the Russian interference in the 2016 US presidential elections. As a method, influence operations offer a relatively easy, cheap and potentially impactful way for instigators to achieve strategic ambitions. Situated in the "gray-zone" between war and peace, influence acts can operate without fearing impactful retributions. Currently, defence against modern influence operations remain in its infancy. Although social media companies and states pertain methods of resistance, a greater synergy between the two is needed at the current stage. Establishing social resilience is most likely the most effective, albeit, also the most comprehensive and difficult method of defence. In the future, influence operations will likely increase in magnitude and complexity aided by more sophisticated "deep fakes", machine learning and computational power. This requires increased attention to the matter. It is thus important to establish a resilient symbiosis between the state, social media companies and the broader society. Overall, engaging in good communication and contributing in the empowerment of resilient narratives offers the greatest insulation to influence operations.

Bibliography

Al-Khatib, Talal. "Hearts and Minds: History of Psychological Warfare." Seeker, April 29, 2015. https://www.seeker.com/hearts-and-minds-history-of-psychological-warfare-1769783167.html.

Alvarez, Lizette. "Radio and TV Martí, U.S. Broadcasters to Cuba, Emerge from Cold War Past Facing Uneasy Future (Published 2015)." *The New York Times*, March 24, 2015, sec. U.S. https://www.nytimes.com/2015/03/25/us/radio-tv-marti-cuba.html.

BBC. "'Post-Truth' Declared Word of the Year by Oxford Dictionaries." *BBC News*, November 16, 2016, sec. UK. https://www.bbc.com/news/uk-37995600#:~:text=Oxford%20Dictionaries%20has%20declared%20%22post.

Bergh, Arild. "Påvirkningsoperasjoner I Sosiale Medier – Oversikt Og Utfordringer." Forsvarets Forskningsinstitutt (FFI), June 17, 2020.

[31] Bruce Schneier, "8 Ways to Stay ahead of Influence Operations," Foreign Policy, August 12, 2019, https://foreignpolicy.com/2019/08/12/8-ways-to-stay-ahead-of-influence-operations/.

———. “Social Network Centric Warfare - Understanding Influence Operations in Social Media.” Norwegian Defence Research Establishment (FFI), October 4, 2019.

Bradshaw, Samantha. “Influence Operations and Disinformation on Social Media.” Centre for International Governance Innovation, November 23, 2020. https://www.cigionline.org/articles/influence-operations-and-disinformation-social-media.

Collins Dictionary. “Collins Word of the Year 2019 Shortlist - Collins Dictionary Language Blog.” Collins Dictionary Language Blog, November 7, 2019. https://blog.collinsdictionary.com/language-lovers/collins-word-of-the-year-2019-shortlist/.

Council of the European Union. “Disinformation during the COVID-19 Pandemic.” www.consilium.europa.eu, July 23, 2020. https://www.consilium.europa.eu/en/documents-publications/library/library-blog/posts/disinformation-during-the-covid-19-pandemic/.

Flood, Alison. “Fake News Is ‘Very Real’ Word of the Year for 2017.” the Guardian. The Guardian, November 2, 2017. https://www.theguardian.com/books/2017/nov/02/fake-news-is-very-real-word-of-the-year-for-2017.

Larson, Eric V., Richard E. Darilek, Daniel Gibran, Brian Nichiporuk, Amy Richardson, Lowell H. Schwartz, and Cathryn Quantic Thurston. “Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities.” *Www.rand.org*, May 27, 2009. https://www.rand.org/pubs/monographs/MG654.html.

Marineau, Sophie. “Fact Check US: What Is the Impact of Russian Interference in the US Presidential Election?” The Conversation, September 29, 2020. https://theconversation.com/fact-check-us-what-is-the-impact-of-russian-interference-in-the-us-presidential-election-146711.

Moy, Wesley R., and Kacper Gradon. “COVID-19 Effects and Russian Disinformation Campaigns.” HOMELAND SECURITY AFFAIRS, December 9, 2020. https://www.hsaj.org/articles/16533.

Mueller, Robert. “Report on the Investigation into Russian Interference in the 2016 Presidential Election.” US Department of Justice, March 2019.

Narula, Sunil. “Psychological Operations (PSYOPs): A Conceptual Overview.” *Strategic Analysis* 28, no. 1 (January 2004): 177–92. https://doi.org/10.1080/09700160408450124.

Nemtsov, Boris. “The Guardian View on Russian Propaganda: The Truth Is out There | Editorial.” the Guardian, March 2, 2015. https://www.theguardian.com/commentisfree/2015/mar/02/guardian-view-russian-propaganda-truth-out-there.

Paul, Christopher. “The Russian ‘Firehose of Falsehood’ Propaganda Model.” Rand.org. RAND Corporation, 2016. https://www.rand.org/pubs/perspectives/PE198.html.

Radio Free Europe RL. “History.” RFE/RL. RFE/RL, May 12, 2019. https://pressroom.rferl.org/history.

Schneier, Bruce. “8 Ways to Stay ahead of Influence Operations.” Foreign Policy, August 12, 2019. https://foreignpolicy.com/2019/08/12/8-ways-to-stay-ahead-of-influence-operations/.

The Reporter. “The Content Mill Empire behind Online Disinformation in Taiwan - 報導者 the Reporter.” www.twreporter.org, December 26, 2019. https://www.twreporter.org/a/information-warfare-business-disinformation-fake-news-behind-line-groups-english.

Thomas, Elise, Natalie Thompson Thompson, and Alicia Wanless. “The Challenges of Countering Influence Operations.” Carnegie Endowment for International Peace, June 10, 2020. https://carnegieendowment.org/2020/06/10/challenges-of-countering-influence-operations-pub-82031.

Weinberg, Dana, and Jessica Dawson. “From Anti-Vaxxer Moms to Militia Men: Influence Operations, Narrative Weaponization, and the Fracturing of American Identity,” 2020. https://doi.org/10.31235/osf.io/87zmk.

Weitz, Richard. “Assessing the Russian Disinformation Campaign during COVID-19.” International Center for Defence and Security, 2020.