Information Operations and Facebook

By Jen Weedon, William Nuland and Alex Stamos

April 27, 2017
Version 1.0

facebook

Version History:
1.0 – Initial Public Release, 27APR2017

Introduction

Civic engagement today takes place in a rapidly evolving information ecosystem. More and more, traditional forums for discussion, the exchange of ideas, and debate are mirrored online on platforms like Facebook – leading to an increase in individual access and agency in political dialogue, the scale and speed of information consumption, as well as the diversity of influences on any given conversation. These new dynamics present us with enormous opportunities, but also introduce novel challenges.

In this context, Facebook sits at a critical juncture. Our mission is to give people the power to share and make the world more open and connected. Yet it is important that we acknowledge and take steps to guard against the risks that can arise in online communities like ours. The reality is that not everyone shares our vision, and some will seek to undermine it — but we are in a position to help constructively shape the emerging information ecosystem by ensuring our platform remains a safe and secure environment for authentic civic engagement.

As our CEO, Mark Zuckerberg, wrote in February 2017:[1]

> *"It is our responsibility to amplify the good effects and mitigate the bad -- to continue increasing diversity while strengthening our common understanding so our community can create the greatest positive impact on the world."*

We believe civic engagement is about more than just voting — it's about people connecting with their representatives, getting involved, sharing their voice, and holding their governments accountable. Given the increasing role that Facebook is playing in facilitating civic discourse, we wanted to publicly share what we are doing to help ensure Facebook remains a safe and secure forum for authentic dialogue.

In brief, we have had to expand our security focus from traditional abusive behavior, such as account hacking, malware, spam and financial scams, to include more subtle and insidious forms of misuse, including attempts to manipulate civic discourse and deceive people. These are complicated issues and our responses will constantly evolve, but we wanted to be transparent about our approach. The following sections explain our understanding of these threats and challenges and what we are doing about them.

1 https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10154544292806634

Information Operations

Part of our role in Security at Facebook is to understand the different types of abuse that occur on our platform in order to help us keep Facebook safe, and agreeing on definitions is an important initial step. We define **information operations**, the challenge at the heart of this paper, as actions taken by organized actors (governments or non-state actors) to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome. These operations can use a combination of methods, such as false news, disinformation, or networks of fake accounts aimed at manipulating public opinion (we refer to these as "false amplifiers").

Information operations as a strategy to distort public perception is not a new phenomenon. It has been used as a tool of domestic governance and foreign influence by leaders tracing back to the ancient Roman, Persian, and Chinese empires, and is among several approaches that countries adopt to bridge capability gaps amid global competition. Some authors use the term 'asymmetric' to refer to the advantage that a country can gain over a more powerful foe by making use of non-conventional strategies like information operations. While much of the current reporting and public debate focuses on information operations at the international level, similar tactics are also frequently used in domestic contexts to undermine opponents, civic or social causes, or their champions.

While information operations have a long history, social media platforms can serve as a new tool of collection and dissemination for these activities. Through the adept use of social media, information operators may attempt to distort public discourse, recruit supporters and financiers, or affect political or military outcomes. These activities can sometimes be accomplished without significant cost or risk to their organizers. We see a few drivers in particular for this behavior:

- **Access - global reach is now possible:** Leaders and thinkers, for the first time in history, can reach (and potentially influence) a global audience through new media, such as Facebook. While there are many benefits to this increased access, it also creates opportunities for malicious actors to reach a global audience with information operations.
- **Everyone is a potential amplifier:** Perhaps most critically, each person in a social media-enabled world can act as a voice for the political causes she or he most strongly believes in. This means that well-executed information operations have the potential to gain influence organically, through authentic channels and networks, even if they originate from inauthentic sources, such as fake accounts.

Untangling "Fake News" from Information Operations

The term "fake news" has emerged as a catch-all phrase to refer to everything from news articles that are factually incorrect to opinion pieces, parodies and sarcasm, hoaxes, rumors, memes, online abuse, and factual misstatements by public figures that are reported in otherwise accurate news pieces. The overuse and misuse of the term "fake news" can be problematic because, without common definitions, we cannot understand or fully address these issues.

We've adopted the following terminology to refer to these concepts:

Information (or Influence) Operations - Actions taken by governments or organized non-state actors to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome. These operations can use a combination of methods, such as false news, disinformation, or networks of fake accounts (false amplifiers) aimed at manipulating public opinion.

False News - News articles that purport to be factual, but which contain intentional misstatements of fact with the intention to arouse passions, attract viewership, or deceive.

False Amplifiers - Coordinated activity by inauthentic accounts with the intent of manipulating political discussion (e.g., by discouraging specific parties from participating in discussion, or amplifying sensationalistic voices over others).

Disinformation - Inaccurate or manipulated information/content that is spread intentionally. This can include false news, or it can involve more subtle methods, such as false flag operations, feeding inaccurate quotes or stories to innocent intermediaries, or knowingly amplifying biased or misleading information. Disinformation is distinct from **misinformation**, which is the inadvertent or unintentional spread of inaccurate information without malicious intent.

The role of "false news" in information operations

While information operations may sometimes employ the use of false narratives or false news as tools, they are certainly not one and the same. There are several important distinctions:

- **Intent**: The purveyors of false news can be motivated by financial incentives, individual political motivations, attracting clicks, or all the above. False news can be shared with or without malicious intent. Information operations, however, are primarily motivated by political objectives and not financial benefit.
- **Medium**: False news is primarily a phenomenon related to online news stories that purport to come from legitimate outlets. Information operations, however, often involve the broader information ecosystem, including old and new media.
- **Amplification**: On its own, false news exists in a vacuum. With deliberately coordinated amplification through social networks, however, it can transform into information operations.

What we're doing about false news

- **Collaborating with others** to find industry solutions to this societal problem;
- **Disrupting economic incentives**, to undermine operations that are financially motivated;
- **Building new products** to curb the spread of false news and improve information diversity; and
- **Helping people** make more informed decisions when they encounter false news.

Modeling and Responding to Information Operations on Facebook

The following sections lay out our tracking and response to the component aspects of information operations, focusing on what we have observed and how Facebook is working both to protect our platform and the broader information ecosystem.

We have observed three major features of online information operations that we assess have been attempted on Facebook. This paper will primarily focus on the first and third bullets:

- **Targeted data collection**, with the goal of stealing, and often exposing, non-public information that can provide unique opportunities for controlling public discourse.[2]
- **Content creation**, false or real, either directly by the information operator or by seeding stories to journalists and other third parties, including via fake online personas.
- **False amplification,** which we define as coordinated activity by inauthentic accounts with the intent of manipulating political discussion (e.g., by discouraging specific parties from participating in discussion or amplifying sensationalistic voices over others). We detect this activity by analyzing the inauthenticity of the account and its behaviors, and not the content the accounts are publishing.

Figure 1: An example of the sequence of events we saw in one operation; note, these components do not necessarily always happen in this sequence, or include all elements in the same manner.

[2] This phase is optional, as content can be created and distributed using publicly available information as well. However, from our observations we believe that campaigns based upon leaked or stolen information can be especially effective in driving engagement.

Targeted Data Collection

Targeted data collection and theft can affect all types of victims, including companies, government agencies, nonprofits, media outlets, and individuals. Typical methods include phishing with malware to infect a person's computer and credential theft to gain access to their online accounts.[3] Over the past few years, there has been an increasing trend towards malicious actors targeting individuals' *personal* accounts - both email and social media - to steal information from the individual and/or the organization with which they're affiliated.

While recent information operations utilized stolen data taken from individuals' personal email accounts and organizations' networks, we are also mindful that any person's Facebook account could also become the target of malicious actors. Without adequate defenses in place, malicious actors who were able to gain access to Facebook user account data could potentially access sensitive information that might help them more effectively target spear phishing campaigns or otherwise advance harmful information operations.

What we're doing about targeted data collection

Facebook has long focused on helping people protect their accounts from compromise. Our security team closely monitors a range of threats to our platform, including bad actors with differing skillsets and missions, in order to defend people on Facebook (and our company) against targeted data collection and account takeover. Our dedicated teams focus daily on account integrity, user safety, and security, and we have implemented additional measures to protect vulnerable people in times of heightened cyber activity such as elections periods, times of conflict or political turmoil, and other high profile events.

Here are some of the steps we are taking:

- Providing a set of customizable security and privacy features[4], including multiple options for two-factor authentication and in-product marketing to encourage adoption;
- Notifications to specific people if they have been targeted by sophisticated attackers[5], with custom recommendations depending on the threat model[6];
- Proactive notifications to people who have yet to be targeted, but whom we believe may be at risk based on the behavior of particular malicious actors;
- In some cases, direct communication with likely targets;
- Where appropriate, working directly with government bodies responsible for election protections to notify and educate people who may be at greater risk.

---

3 https://www.secureworks.com/research/threat-group-4127-targets-google-accounts

4 https://www.facebook.com/help/325807937506242/, https://www.facebook.com/help/148233965247823

5 https://www.facebook.com/notes/facebook-security/notifications-for-targeted-attacks/10153092994615766/

6 We notify our users with context around the status of their account and actionable recommendations if we assess they are at increased risk of future account compromise by sophisticated actors or when we have confirmed their accounts have been compromised.

False Amplifiers

A false amplifier's[7] motivation is ideological rather than financial. Networks of politically-motivated false amplifiers and financially-motivated fake accounts have sometimes been observed commingling and can exhibit similar behaviors; in all cases, however, the shared attribute is the inauthenticity of the accounts. False amplifier accounts manifest differently around the globe and even within regions. In some instances dedicated, professional groups attempt to influence political opinions on social media with large numbers of sparsely populated fake accounts that are used to share and engage with content at high volumes. In other cases, the networks may involve behavior by a smaller number of carefully curated accounts that exhibit authentic characteristics with well-developed online personas.

The inauthentic nature of these social interactions obscures and impairs the space Facebook and other platforms aim to create for people to connect and communicate with one another. In the long-term, these inauthentic networks and accounts may drown out valid stories and even deter some people from engaging at all.

While sometimes the goal of these negative amplifying efforts is to push a specific narrative, the underlying intent and motivation of the coordinators and sponsors of this kind of activity can be more complex. Although motivations vary, the strategic objectives of the organizers generally involve one or more of the following components:

- **Promoting or denigrating a specific cause or issue**: This is the most straightforward manifestation of false amplifiers. It may include the use of disinformation, memes, and/or false news. There is frequently a specific hook or wedge issue that the actors exploit and amplify, depending on the targeted market or region. This can include topics around political figures or parties, divisive policies, religion, national governments, nations and/or ethnicities, institutions, or current events.
- **Sowing distrust in political institutions**: In this case, fake account operators may not have a topical focus, but rather seek to undermine the status quo of political or civil society institutions on a more strategic level.
- **Spreading confusion**: The directors of networks of fake accounts may have a longer-term objective of purposefully muddying civic discourse and pitting rival factions against one another. In several instances, we identified malicious actors on Facebook who, via inauthentic accounts, actively engaged across the political spectrum with the apparent intent of increasing tensions between supporters of these groups and fracturing their supportive base.

[7] A fake account aimed at manipulating public opinion.

What does false amplification look like?

- Fake account creation, sometimes en masse;
- Coordinated sharing of content and repeated, rapid posts across multiple surfaces (e.g., on their profile, or in several groups at once);
- Coordinated or repeated comments, some of which may be harassing in nature;
- Coordinated "likes" or reactions;
- Creation of "astroturf"[8] groups. These groups may initially be populated by fake accounts, but can become self-sustaining as others become participants;
- Creation of Groups or Pages with the specific intent to spread sensationalistic or heavily biased news or headlines, often distorting facts to fit a narrative. Sometimes these Pages include legitimate and unrelated content, ostensibly to deflect from their real purpose;
- Creation of inflammatory and sometimes racist memes, or manipulated photos and video content.

There is some public discussion of false amplifiers being solely driven by "social bots," which suggests automation. In the case of Facebook, we have observed that most false amplification in the context of information operations is not driven by automated processes, but by coordinated people who are dedicated to operating inauthentic accounts. We have observed many actions by fake account operators that could only be performed by people with language skills and a basic knowledge of the political situation in the target countries, suggesting a higher level of coordination and forethought. Some of the lower-skilled actors may even provide content guidance and outlines to their false amplifiers, which can give the impression of automation.

This kind of wide-scale coordinated human interaction with Facebook is not unique to information operations. Various groups regularly attempt to use such techniques to further financial goals, and Facebook continues to innovate in this area to detect such inauthentic activity.[9] The area of information operations does provide a unique challenge, however, in that those sponsoring such operations are often not constrained by per-unit economic realities in the same way as spammers and click fraudsters, which increases the complexity of deterrence.

Figure 2: Example of repeated posts in various groups

[8] Organized activity that purports to reflect authentic individuals but is actually manufactured, as in "fake grass-roots."

[9] https://www.facebook.com/notes/facebook-security/disrupting-a-major-spam-operation/10154327278540766/

What we're doing about false amplification

Facebook is a place for people to communicate and engage authentically, including around political topics. If legitimate voices are being drowned out by fake accounts, authentic conversation becomes very difficult. Facebook's current approach to addressing account integrity focuses on the authenticity of the accounts in question and their behaviors, not the content of the material created.

Facebook has long invested in both preventing fake-account creation and identifying and removing fake accounts. Through technical advances, we are increasing our protections against manually created fake accounts and using new analytical techniques, including machine learning, to uncover and disrupt more types of abuse. We build and update technical systems every day to make it easier to respond to reports of abuse, detect and remove spam, identify and eliminate fake accounts, and prevent accounts from being compromised. We've made recent improvements to recognize these inauthentic accounts more easily by identifying patterns of activity — without assessing account contents themselves.[10] For example, our systems may detect repeated posting of the same content, or aberrations in the volume of content creation. In France, for example, as of April 13, these improvements recently enabled us to take action against over 30,000 fake accounts.[11]

Figure 3: An example of a cluster of related accounts used for false amplification.

10 https://www.facebook.com/notes/facebook-security/improvements-in-protecting-the-integrity-of-activity-on-facebook/10154323366590766/

11 This the figure announced in our last security note. We expect this number to change as we finish deploying these improvements and continue to stay vigilant about inauthentic activity.

A Deeper Look: A Case Study of a Recent Election

During the 2016 US Presidential election season, we responded to several situations that we assessed to fit the pattern of information operations. We have no evidence of any Facebook accounts being compromised as part of this activity, but, nonetheless, we detected and monitored these efforts in order to protect the authentic connections that define our platform.

One aspect of this included malicious actors leveraging conventional and social media to share information stolen from other sources, such as email accounts, with the intent of harming the reputation of specific political targets. These incidents employed a relatively straightforward yet deliberate series of actions:

- Private and/or proprietary information was accessed and stolen from systems and services (outside of Facebook);
- Dedicated sites hosting this data were registered;
- Fake personas were created on Facebook and elsewhere to point to and amplify awareness of this data;
- Social media accounts and pages were created to amplify news accounts of and direct people to the stolen data.
- From there, organic proliferation of the messaging and data through authentic peer groups and networks was inevitable.

Concurrently, a separate set of malicious actors engaged in false amplification using inauthentic Facebook accounts to push narratives and themes that reinforced or expanded on some of the topics exposed from stolen data. Facebook conducted research into overall civic engagement during this time on the platform, and determined that the reach of the content shared by false amplifiers was marginal compared to the overall volume of civic content shared during the US election.[12]

In short, while we acknowledge the ongoing challenge of monitoring and guarding against information operations, the reach of known operations during the US election of 2016 was statistically very small compared to overall engagement on political issues.

Facebook is not in a position to make definitive attribution to the actors sponsoring this activity. It is important to emphasize that this example case comprises only a subset of overall activities tracked and addressed by our organization during this time period; however our data does not contradict the attribution provided by the U.S. Director of National Intelligence in the report dated January 6, 2017.[13]

---

[12] To estimate magnitude, we compiled a cross functional team of engineers, analysts, and data scientists to examine posts that were classified as related to civic engagement between September and December 2016. We compared that data with data derived from the behavior of accounts we believe to be related to Information Operations. The reach of the content spread by these accounts was less than one-tenth of a percent of the total reach of civic content on Facebook.

[13] https://web-beta.archive.org/web/20170421222356/https://www.dni.gov/files/documents/ICA_2017_01.pdf

The Need for Wider Efforts

Information operations can affect the entire information ecosystem, from individual consumers of information and political parties to governments, civil society organizations, and media companies. An effective response, therefore, requires a whole-of-society approach that features collaboration on matters of security, education, governance, and media literacy. Facebook recognizes that a handful of key stakeholder groups will shoulder more responsibility in helping to prevent abuse, and we are committed not only to addressing those components that directly involve our platform, but also supporting the efforts of others.

Facebook works directly with **candidates, campaigns, and political parties** via our political outreach teams to provide information on potential online risks and ways our users can stay safe on our platform and others. Additionally, our peers are making similar efforts to increase community resources around security.[14] However, it is critical that campaigns and parties also take individual steps to enhance their cybersecurity posture. This will require building technical capabilities and employing specific industry-standard approaches, including the use of cloud options in lieu of vulnerable self-hosted services, deploying limited-use devices to employees and volunteers, and encouraging colleagues, friends, and family to adopt security practices like two-factor authentication. Individual campaigns may find it difficult to build security teams that are experienced in this level of defense, so shared managed services should be considered as an option.

Governments may want to consider what assistance is appropriate to provide to candidates and parties at risk of targeted data theft. Facebook will continue to contribute in this area by offering training materials, cooperating with government cybersecurity agencies looking to harden their officials' and candidate's social media activity against external attacks, and deploying in-product communications designed to reinforce observance of strong security practices.

Journalists and news professionals are essential for the health of democracies. We are working through the Facebook Journalism Project[15] to help news organizations stay vigilant about their security.

In the end, societies will only be able to resist external information operations if all citizens have the necessary media literacy to distinguish true news from misinformation and are able to take into account the motivations of those who would seek to publish false news, flood online forums with manipulated talking points, or selectively leak and spin stolen data. To help advance media literacy, Facebook is supporting **civil society programs** such as the News Integrity Coalition to improve the public's ability to make informed judgments about the news they consume.

[14] https://medium.com/jigsaw/protect-your-election-helping-everyone-get-the-full-story-faea40934dd2
[15] https://media.fb.com/2017/01/11/facebook-journalism-project/

Conclusion

Providing a platform for diverse viewpoints while maintaining authentic debate and discussion is a key component of Facebook's mission. We recognize that, in today's information environment, social media plays a sizable role in facilitating communications — not only in times of civic events, such as elections, but in everyday expression. In some circumstances, however, we recognize that the risk of malicious actors seeking to use Facebook to mislead people or otherwise promote inauthentic communications can be higher. For our part, we are taking a multifaceted approach to help mitigate these risks:

- Continually studying and monitoring the efforts of those who try to negatively manipulate civic discourse on Facebook;
- Innovating in the areas of account access and account integrity, including identifying fake accounts and expanding our security and privacy settings and options;
- Participating in multi-stakeholder efforts to notify and educate at-risk people of the ways they can best keep their information safe;
- Supporting civil society programs around media literacy.

Just as the information ecosystem in which these dynamics are playing out is a shared resource and a set of common spaces, the challenges we address here transcend the Facebook platform and represent a set of shared responsibilities. We have made concerted efforts to collaborate with peers both inside the technology sector and in other areas, including governments, journalists and news organizations, and together we will develop the work described here to meet new challenges and make additional advances that protect authentic communication online and support strong, informed, and civically engaged communities.

About the Authors

Jen Weedon is the manager of Facebook's Threat Intelligence team and has held leadership roles at FireEye, Mandiant, and iSIGHT Partners. Ms. Weedon holds an MA in International Security Studies from the Fletcher School at Tufts University and a BA in Government from Smith College.

William Nuland is an analyst on the Facebook Threat Intelligence team and has worked in threat intelligence at Dell SecureWorks and Verisign iDefense. Mr. Nuland holds an MA from the School of Foreign Service at Georgetown University and a BA in Comparative Literature from NYU.

Alex Stamos is the Chief Security Officer of Facebook, and was previously the CISO of Yahoo and co-founder of iSEC Partners. Mr. Stamos holds a BS in Electrical Engineering and Computer Science from the University of California, Berkeley.