Social Media: An Evolving Front in Radicalization

J.M. Berger

Non-resident fellow, Project on U.S. Relations with the Islamic World

The Brookings Instititition

The self-styled Islamic State, also known as ISIL or ISIS, is not the first group to employ social media as a tool for recruitment and propaganda, but its innovative and aggressive approach has afforded it an unprecedented level of success, and its activities will likely provide a template for future extremist initiatives.

Since the beginning of 2015, at least 30 Americans in 13 states have been subject to law enforcement action for attempting to join ISIS or carry out violence inspired by ISIS. In every case, a significant social media component was found in the radicalization or recruitment process.

In cases where a clear trajectory could be determined, about one-third of the suspects appear to have been radicalized by al Qaeda-affiliated content prior to the rise of ISIS, and only later shifted allegiance to the Islamic State. The remainder were reportedly radicalized by ISIS directly. While this points to the growing influence of ISIS among those vulnerable to radicalization, it also highlights the fact that this activity takes place in an evolving context, rather than being an entirely new or different problem.

While trends can be detected, those radicalized continue to defy generalization. The majority of those charged were males under the age of 30, but almost 20 percent were women and approximately 30 percent were older than 30. About 30 percent of the cases involved some discussion of a violent plot in the United States, with most of the remainder involving efforts to travel to Syria and join ISIS there.

The role of global social media has made it possible for adherents of even the most outlying extremist ideologies to connect and communicate. In addition, the increasing ease of global travel makes it possible for the most committed and fanatical to gather in specific geographical locations.

Furthermore, a proliferation of technologies for inflicting mass casualties empower those who are frustrated in their efforts to travel to Iraq and Syria to act violently at home, often with outsized consequences that echo through the 24-hour news cycle.

In the blunt numerical context of a world with 7 billion people or a Twitter monthly active user base of 302 million, active supporters of ISIS barely register. They represent a fraction of 1 percent of Muslims worldwide, and an even smaller fraction of the world's population.

But when adherents of a violent ideology can connect and communicate swiftly and easily, these tiny percentages add up to hundreds or even thousands of people who can congregate or act in loose concert, exerting a disproportionate impact on global politics and world events. Social media is a critical tool for organizing such activity.

There are three major components to ISIS's social media campaign.

The first is disseminating propaganda to generate support for the group and attract potential recruits and supporters locally and abroad.

The second is disseminating propaganda designed to manipulate its enemies' perceptions and political reactions. While some of this material purports to demoralize and deter potential enemies from taking action, its real intent is often to inflame animosity and engage foreign countries in a wider regional war. Some of this propaganda also aims to undermine the unity of the coalition opposing ISIS. Its terrorist actions are synchronized with this goal.

The third major component is recruitment. Here, the broad strokes of ISIS's highly visible propaganda campaign give way to a host of smaller, individualized activities.

Due to its unusually large size (in the context of extremist groups) and its large contingent of foreign fighters, ISIS can attack the recruiting problem using a wide variety of tactics, with staffing levels that allow for a very high ratio of radicalizers to potential recruits.

ISIS has cultivated recruiters and radicalizers who speak the native languages of Western countries. In some cases, as in Minnesota, supporters and recruiters work on the ground and synchronize their bricks-and-mortar operations with online outreach. In other cases, it pursues purely online initiatives, benefiting from the sense of remote intimacy that comes with constant contact using always-on media.

These approaches are detectable in open sources, up to a point, although recruits who reach a critical decision-making stage are often shifted off of public social media platforms such as Twitter and Facebook to private social media such as Kik and WhatsApp, where interactions cannot be directly observed using open-source tools.

In Garland, Texas, on May 3, 2015, two apparent ISIS supporters were killed attempting to attack an event that involved drawing the Prophet Mohammed. A police officer was wounded.

ISIS supporters online had openly urged attacks on the event for more than a week prior, and while the attack was thwarted, it was not prevented.

The challenge in such cases is separating the signal from the noise. ISIS supporters online generate a very substantial amount of noise, yet it is relatively uncommon for a specific attack to be so clearly reflected in data preceding its execution. Therefore caution should be exercised when relying on open-source intelligence to anticipate attacks. ISIS supporters are likely to become more vocally threatening if they believe U.S. law enforcement will allocate resources every time they name a specific target.

The increasing disruption of ISIS’s most visible propaganda activities -- on platforms such as YouTube, Facebook, and increasingly Twitter -- has decreased its ability to broadcast its message to the widest possible audiences. The crackdown by social media providers has created tradeoffs in detecting recruitment.

When broader propaganda efforts are disrupted, recruitment increasingly shifts to a peer-to-peer model of individual relationships. For instance, one of the most commonly observed interactions involves foreign fighters in Syria speaking directly to vulnerable young people in the U.S. using private Facebook messages. This activity is harder to detect in open-source, but not necessarily impossible. New and better techniques are needed to identify both recruiters and at-risk populations.

But while detection and interdiction for purposes of countering violent extremism become more labor-intensive as a result of suspensions, these disruptions also increase the amount of time and energy ISIS must expend to find and attract new recruits. Adherents are persistent in returning to the field with new accounts, an activity that can be countered more effectively but probably cannot be entirely defeated. The bottom line: Extremist activity on social media cannot be eliminated, it can only be weakened.

Current efforts to counter ISIS activity are inhibited by two key challenges.

The first is commitment. ISIS supporters rarely tire of promoting their message, and they are not easily deterred. Faced with an aggressive spike in suspensions on Twitter, they have mounted a variety of labor-intensive countermeasures that keep them in the game, albeit at a reduced level.

The process of reporting pro-ISIS users for suspension requires a steady and ongoing commitment. Twitter suspensions are reportedly based primarily on user reporting of abusive content. If the reporters get bored or distracted, the network gains time to regenerate. Only a consistent effort will produce a consistent result, but the current level of pressure is certainly having some effect.

This leads us to the second challenge, which is the near total outsourcing of anti-ISIS activity online. To date, the vast majority of Twitter abuse reporting is apparently done by hacktivists. The largest and most organized efforts to counter ISIS online, either through reporting or the spread of competing messages, include:

- "Anonymous," an amorphous collection of anonymous vigilantes, including significant numbers who engage in unrelated illegal or antigovernment activities.
- Foreign and domestic activist networks and political groups that are predicated on anti-Muslim sentiment, at times including the language of overt bigotry.
- Foreign government influence operations, such as Russian, Syrian and Iranian programs, whose operations include substantial activity adversarial to U.S. foreign policy and inimical to our national security.
- Other hacktivists of unknown origin who deploy spam techniques and malware against ISIS online. Recent examples include content that appears to originate in Japan and Saudi Arabia, but may be deliberately misleading as to its origins.

Similar to the bricks-and-mortar military coalition against ISIS, members of these networks have a variety of motives for participating, not all of them consistent with American values, or our security and foreign policy goals.

A great many Muslim voices oppose ISIS and its values on a daily basis, however these efforts tend to be organic, rather than highly organized campaigns, especially in English. While such individual voices are crucially important, Muslims seeking to counter ISIS should also pursue more organized strategies. Within the Muslim-American community, programs are already in development to address this gap.

If the U.S. government wishes to directly counter ISIS online, such initiatives will require latitude to engage in trial and error. Programs must be prepared to produce and disseminate extremely high volumes of content. In the current political environment, where back-seat drivers and courters of controversy are found in abundance, this is a difficult proposition.

Government efforts are also subject to limitations on how we conduct information operations, or more bluntly, propaganda. Liberal democracies require that such operations be truthful and acknowledge the concerns of multiple constituencies. And activities undertaken on social media, especially in English, are subject to high levels of scrutiny and instant critique.

Any efforts to move forward in this space must create opportunities for experimentation and allow room for missteps. I am not optimistic that this administration and this Congress are capable of giving a government agency the latitude necessary to successfully undertake a more aggressive approach.

Unfortunately, this means the burden falls on volunteers, activists and community groups. As noted above, private sector players who are currently most active in countering ISIS bring a lot of baggage to the process. Furthermore, private sector groups often lack the funding and manpower needed to be effective. ISIS deploys thousands of activists to promote its messages on a daily basis. To be effective against ISIS, we must be prepared to deploy similar numbers.

Some of the limitations I have discussed here may be surmountable. If they are not, we are left with relatively few options.

First, we can continue under the current scenario, which is already having a detrimental effect on the performance of ISIS online networks.

Second, we can find ways to incentivize private sector participation in anti-ISIS initiatives. There are considerable complications here, including the fact that government support (either moral or financial) can delegitimize organizations working to counter violent extremism in the eyes of their target audiences. The government's expectations of potential partners also limit the field. For instance, it is doubtful government-supported activists would be permitted to engage in frank discussions about politically sensitive U.S. policies that are important to target audiences.

Third, we can create government information programs that involve a large number of accounts focused on generating substantial volumes of anti-ISIS activity online, while taking a conservative and limited approach to the content. As the example of Russian online propaganda demonstrates, there are benefits to simply injecting noise into contested online spaces, but such efforts must take place at a very fast tempo in order to have an effect. A modest success in this space may also help pave the way for more innovative efforts in the future.

Fourth, we can deploy intelligence and other reporting assets to expose the current standard of living within ISIS territories. Recent news reports suggest deteriorating conditions in major centers such as Raqqa and Mosul, but these are based mainly on eyewitness accounts. To counter ISIS's highly visual propaganda, we must obtain and distribute images and video that undermines its extensive propaganda depiction of a high-functioning state. This step is critical to undercutting ISIS's powerful millenarian appeal.

In conclusion, it is important to remember that the study of social media is relatively new and rapidly evolving. Unpredictable outcomes are inevitable in highly interconnected networks. While social network analysis offers great promise as a way to understand the world, we are still at an early stage in determining which approaches work. ISIS's social media campaign has evolved and adapted significantly over the course of its short history, and if we seek to meet them on the online battlefield, we must do the same.