The Dark Side of Social Media: Did Facebook, Twitter and YouTube Kill Charlie?

Terrorists actively use social media networks to spread their propaganda and recruit fighters as well as copycats. Should social media be regulated and, if so, how?

The deadly terrorist attacks on Paris in early January triggered an unprecedented movement of protests throughout the world, from peaceful protests in Paris in support of the victims to more recent counter protests in Arab countries against the new edition of Charlie Hebdo. 2015 has barely started, and social media are already raging. The role of social media behind such movements is not new – their ability to shape social movements has long been recognised; what the recent events have sadly shown is that social media have become a cornerstone of extremist groups' strategies. Put simply, more than being an ideological battleground, social media now act as the backbone of extremists' organisations, with the deadly consequences that we know.

How do extremists leverage social media?

If there is one topic all experts invited to comment on the attacks agree about, it is the fact that extremists are really good - significantly better than most businesses or states - in their use of social media. For instance, Islamic State (IS) has become a master at social media communication, from content creation and communication. It publishes four to five videos per week, with content that is easy to understand, often extreme and/or practical, increasing its potential to become viral. It explains its strategy to potential recruits, using new recruits as brand ambassadors. They **tweet selfies from the desert** in Syria, and post photos of luxuries such as Red Bull with the hashtag #FiveStarJihad. They post threats to their home countries with emoticons and internet acronyms to appeal to the young and restless back home.

They also use their hostages to spread the word. Journalist **John Cantlie**, kept hostage in Syria, has been "used" to present a series of "documentaries", in reality pro-regime propaganda. The IS media machine also conducts illegal activities, such as shutting down or **hacking** social media platforms of their enemies, such as the Central Command, the U.S. military command covering the Middle East. Ironically, a recent hack immediately followed a press conference led by U.S. President Obama around **cyber security legislation** asking companies to tell their clients as soon as they suffered a data breach.

They also mix online and offline propaganda. To illustrate, Al-Qaeda in the Arabian Peninsula (AQAP) has published a newspaper since 2010, "Inspire", that complements their social media propaganda. They use the whole range of digital channels with dexterity, from YouTube to expose their ideas and create powerful images to more intimate chat rooms and forums (for example, ask.fm) to finish persuading potential recruits.

Incidentally, other terrorists, such as Anders Behring Breivik, the white supremacist responsible for the murder of 77 people in 2011 in Norway, has something in common with Islamic extremists; an obsession with technology and the knowledge to use it for the biggest impact.

Where Social Media Really Helps Them

The multichannel communications campaign mounted by terrorist organisations has helped them to raise awareness much faster than conventional means. Potential recruits are noticed and groomed in online forums often based on personality factors. Their messages are widely seen, which help them to spread their ideas even faster.

They create a sense of deep engagement by constantly pushing out content. And they structure their communities quickly, tapping into the three core components of communities:

1. A language: through a variety of formats and spokespeople, they establish a jargon (keywords that support their propaganda, ideology and enhance their communication).
2. A set of core motives: they can also channel their potential supporters' motivations through misleading content. In some cases, IS propaganda also relies on the target imagery; for instance, mixing IS fighters with the imagery of heroes in games (they tell people "you'll be a super hero" and mix the imagery of the game heroes with that of IS fighters).
3. A set of interactions: they create celebrations and rituals, for instance through forums as a means to structure a community to reach their goals (for example, terrorist attacks).

What Should Change? Ethical and Financial Challenges to Come

Of course, no social media platform is directly responsible for the recent attacks or any other terrorist attacks for that matter. Putting all the blame on Facebook, Twitter or YouTube would be nonsense. However, this does not preclude policy makers from examining together with the major actors whether and how new steps might be taken to effectively counter cyber attacks and propaganda. In fact France's Interior Minister Bernard Cazeneuve, along with Germany and the U.K., is currently engaging with Google, Facebook and others to examine what should change, if anything. At an abstract level, the cyber threats ask three fundamental questions: (1) How to balance freedom of expression and the prevention and monitoring of extreme groups and tools? (2) Who should be in charge of countering extreme propaganda? (3) What tools should be used to counter extreme propaganda? The answers are not obvious, but we need to start this conversation.

Of course, shutting down social media sites would be extreme in itself, as we would only limit our own ability to express ourselves and lose the ability to track extremist groups on social media. Besides, it is very difficult to decide (on what basis) what content might be in the "red zone" or not although this could be considered within a broad code of ethics or general agreed-upon frameworks to follow. Europe has already set a precedent with the "right to be forgotten", which now gives users the ability to request removal of content that may damage their reputation. And these requests are not absolute, but are **balanced against other fundamental rights**, "such as freedom of expression and of the media", according to the European Commission.

Another solution for social media sites or search websites that are rich in big data could be to provide balanced or contradictory content more systematically. What if, instead of purely removing content, content judged "dangerous" would automatically be juxtaposed and presented with counter content? Some sites already have teams that review content all day and ban content if needed, but this might not be enough. Social media websites might need to rethink how to present and facilitate information sharing. After all, some websites already present two-sided information – (for example, e-commerce or booking websites such as TripAdvisor where positive and negative reviews help consumers make better informed decisions). To what extent could this be leveraged?

Another important question, as groups under attack are very diverse, lies in how victims can protect themselves and engage in cyber-protection – victims (like Charlie Hebdo) are typically small and do not have the ability to form a cyber team. This is very different from large businesses and strong brands that, when attacked by activists, have the structure and financial means to effectively counter-attack. This debate must happen at a wider scale (for example, unions or national states). Also, national states might decide to be more proactive in actively combating extremist ideas, above and beyond merely listening to sources. Because enrolment of the youth is often the first ladder to a dangerous cycle, more resources need to be devoted to deconstructing the messages the youth are exposed to. To illustrate, France has recently increased the funding of pedagogical initiatives (including cyber-pedagogy) aimed at creating mass production of counter arguments and tools against persuasive communications from certain extreme groups and will grow from 250 to more than a 1,000 specialised policemen to counter cyber attacks.

Where should this battle take place, and to what

extent should social media platforms initiate the change? Facebook, Twitter and YouTube have become the battleground whether they like it or not. Most of them started with the promise of increasing freedom and possibilities; now that it is at stake, and it is a matter of national security, their next step might very well entail leveraging technology to build more critical and informed citizens and consumers. At least, the opportunity is there. What stakeholders should be involved? How restrictive should the new policies be? How to best remodel the platforms? And should we regulate such platforms? At last, the conversation is starting.

David Dubois *is an Assistant Professor of Marketing at INSEAD. Follow David on Twitter* ***@d1dubois****.*

Joerg Niessing *is an Affiliate Professor of Marketing at INSEAD. You can follow Joerg on Twitter* ***@JoergNiessing***

Find article at
https://knowledge.insead.edu/blog/insead-blog/the-dark-side-of-social-media-did-facebook-twitter-and-youtube-kill-charlie-3804