COUNTERING ONLINE RADICALIZATION - LESSONS LEARNED

Daniela ŞTEFĂNESCU, Teodoru ŞTEFAN

'Mihai Viteazul'National Intelligence Academy, Bucharest, Romania

Abstract: *A feature of contemporary conflicts is the increasing number of actors who are willing and able to create both online and offline effects through online activities, and social media are an integrated part thereof. To that end, social media was used by terrorists as recruitment, propaganda, and information tool and the intelligence structures had to find the necessary awareness programs to react to. In this paper we tried to make an analysis of some national awareness strategies (the US, the UK, France, Italy, and Germany ones) in order to set up a guideline of the positive results registered by some countries in this field.*

Keywords*: awareness; radicalization; intelligence; social media; lessons learnt*

1. CONTEXT

Availability of personal, commercial and public sector information and the potential use of infrastructure and control systems represent new sources of vulnerability for society, exacerbated by the growing use of mobile devices and wireless networks, including by a number of non-state actors like Al-Qaeda, Boko Haram, Daesh, Al Murabitoune or other terrorist groups. Technological development has led to the emergence of new types of actors in addition to traditional state actors and probably non-state actors (for example, rebel movements and terrorist organizations), such as online activist groups and corporate entities starting to become direct participants in conflict. To that end, one of the contemporary conflicts feature is the increasing number of actors who are willing and able to create both online and offline effects through cyber activities and social media are an integral part of this process being used by all kind of ill-intended persons including terrorists. In order to understand and counter their actions the intelligence services have develop specific programs aimed mainly at finding the way to react to radicalization and counter its effects. As far as the online radicalization is concerned, many times the strategy to counter this phenomenon included both cyber actions and awareness programs. The last ones are part of the communications strategy the intelligence services are promoting and this is why we considered important to underline the communication framework first and then to present the methods used to counter online radicalization.

2. COMMUNICATION STRATEGIES

A look on the public activities of the intelligence services in the US, the UK, France, Germany, and Italy has revealed some cases in which the use of communication strategies can be subsumed to the concept of awareness. They can be segregated according to the type of communication chosen in two categories influenced, most likely, by the socio-cultural features of each state: direct communication (the US, Germany) and the indirect one (the UK, France and Italy).

The main element for making the differences is given by the action model: organization, types of used instruments, and types of activities, target audience, as well as consistency of the send institutional messages. Thus, the US intelligence services rely on "Hollywood Style" communication. Relevant here is the collaboration with the entertainment industry, and also the extensive exploitation of technological tools in the field of communication (websites, social platforms, video sharing and photo platforms).

On the other hand, European services (from the UK, France, Germany and Italy) resort to communication through the media. In particular, the German intelligence services act together in order to fulfill the stated objective of building a profile of the institutions deeply rooted in the social system, essential for modern professional services. Whatever the type of speech practiced, the activities, the techniques or tools used there are some common trends in terms of services public communication that focus resources towards achieving the specific objectives which we will explain below.

2.1 Institutional Values and Mission Promotion. Official websites, social platforms continue to be used as instruments by American and British services, along with prestigious media outlets (Forbes, Washington Post / the US Financial Times, Daily Telegraph, The Guardian / the UK, Le Nouvel Observateur, Le Point, Le Monde / France). Communicators come mainly from the institutional leadership and their appearances are limited: occasional interviews in prestigious publications on specific occasions (after terrorist attacks, the capture of some terrorist), statements at conferences / debates involving the participation of the institutions they represent or on the services' sites. Complementary activities are undertaken: awareness campaigns, "open doors" events, films, publications, brochures, newsletters.

2.2. Security Culture Dissemination. In the US, CIA is an example of the efforts to promote security culture, including on online radicalization topics, and many tools are used in order to deliver the message that develop social responsibility from programs for parents and children to support to the work of some foundations. FBI has also the Safe Online Surfing Internet Challenge program for pupils and students to learn how to recognize and respond to cyber threats and online radicalization signs. In Italy, some similar efforts were launched by the Department of Information Security and were aimed at primary and secondary pupils.

In this respect, one should also take into consideration German services concerted actions on two relevant components for the security education: understanding intelligence as a social mission and emphasizing the role of history in order to help employees identify themselves with their work and tasks. We also note the strategy used by German services to send institutional messages through: participation in events organized by associations / foundations / civil society organizations or official institutions; exhibitions, conferences, symposium on threats to national security.

Taking into account these strategies we note that European states have understood the need to strengthen public trust as far as intelligence services and state institutions are concerned, while US Administration still adopts a direct approach toward the audience.

3. COUNTER RADICALIZATION STRATEGIES

The dangers of online terrorist narrative caused a series of counter-measures implemented by governments and international organizations that can be classified into two types: repressive and soft measures. The repressive measures are focused on denying access/spread of extremist messages by terrorist organizations and their supporters by blocking sites and prohibiting message or communication spreading radical content and thus prosecute those who propagate it. Worldwide efforts have been made to counter Daesh messages. The response of governments and corporations focused on "blocking strategy", meaning they suspended numerous supporters Daesh accounts on Twitter, YouTube, Facebook and other Internet content platforms. The method has a limited effect because it is very easy to set up new sites unknown to authorities. Deleted accounts are opened again under other names, gaining more followers and even a higher level of legitimacy and celebrity.

Intelligence collection works hand-in-hand with the removal of content, as practiced by the 'Check the Web' portal, an EU database created in 2007 to map jihadist online activities. The intelligence-led approach has proven to be very successful if ordinary internet users were made part of the process, as in the case of the wannabe assassin who plotted to kill Macron, whose chat messages were reported by anonymous internet users to Pharos, the French online portal designed to prompt government action by investigating the authenticity and threat level of reported messages and online content.

At the EU level, among the most notable efforts is the creation of the Radicalisation Awareness Network (RAN) in 2012 and especially RAN's Communication and Narrative Working Group that focuses on creating communication and counter-messaging strategies to challenge extremist content online. As far as the soft measures are concerned, the main strategy used is the counter narrative and strategic communication. There are several categories of strategic communication which addresses how actors can respond to jihadist organizations narrative and the activities of jihadist organizations are covered in media. The first one relates to public information campaigns about Western involvement in the conflict and aims at explaining foreign policy on sensitive issues and promoting an alternative discourses about Western values. Such alternative messages are the UK "Radical Middle Way" program, created after the 7 July 2005 attacks on London's transport systems, and the US public education campaign "MyJihad".

Another element of strategic communication is counter narrative. Among the examples we mention the US campaigns "Say No to Terror" and "Think again, turn away", the Australian @Fight_DAESH program, as well as the #notanotherbrother of the British Quilliam Foundation.

All these programs have been tailored to take into account the developments in security environment and national risks posed by the impact of radicalization process. Therefore, in some cases the intelligence services adopted their communication strategies to include ways to counter radicalization, especially as part of their counter terrorism strategy.

Following the terrorist attacks in 2015, the French government launched the stop-djihafisme.gouv.fr online platform dedicated to preventing and combating terrorism among radicalized young people or those at the risk of being radicalized. In the same year, it launched a hotline available from Monday to Friday between 09:00-17:00 where people can call if they detect any danger of radicalization at someone they know.

Nowadays the hotline is a common method that is used by all intelligence services and the contact data can be find on their websites or social media platforms. Sometimes the intelligence services adopted the methods they already have been using for other purposes. Thus, since 2007, Germany has implemented, at the federal and also regional level and in particular by the Federal Office for the Protection of the Constitution/BfV, a series of information campaigns on the risks to security, focusing on the cyber and extremist ones, and lately they included online terrorism.

Another aspect to be considered was the establishment of some institutional platforms of expertise. Thus, the National Center for Countering Cyber Attacks/NCAZ[1] was established in February 2011 in Bonn.

BSI has published several issues on cyber security and countering online radicalization for programs/projects of research and development. One of these is *IT-Grundschutz* an educational and professional training program aimed to increase public awareness, promote cyber security courses in higher education and certification of professionals in the public and private sectors. In September 2013, BfV established *Hatifa* program (Arabic translation phone, an acronym for *Heraus und Aus Terrorismus IslamistichemFanatismus*) which aims to help people who want to leave terrorist or extremist organizations. Thus, any person who wishes to be deradicalized can call or email BfV and a specialist will provide him psychological counseling. In order to support national radicalization programs from 2014 the lands of Hesse, Hamburg, Lower Saxony, Bavaria, and Baden-Wurttemberg launched the *Violence Prevention Network*, based in Frankfurt, whose mission is to advise young radicalized people and their friends, families, teachers or colleagues.

The success of this approach was translated at the EU level and led to the creation of the *European Network of Radicalization* (EnoD), an interactive platform consisting of NGOs directly involved in the deradicalization actions conducted by various Member States (Austria, Czech Republic, Denmark, Finland, Germany, France, Ireland, Italy, Britain, Poland, Slovakia, the Netherlands, Sweden, and Hungary). NGO activists regularly meet to exchange information on methods used, target groups, criteria for best practices, difficulties and support received from Member States.

The US changed the way in which it delivers countering terrorist narratives moving from a direct to an indirect approach, and focusing on facilitating other actors with more credible voices to deliver messages. In previous years, it had attempted to counter terrorist narratives directly, through the Center for Strategic Counterterrorism Communications (CSCC), whereas it now often takes the role of facilitator through the Global Engagement Center (GEC), encouraging other counter narrative organizations, such as the Sawab Center and Regional Digital Counter-Messaging Communication Center (RDC3), to become the messenger.

4. POTENTIAL GUIDELINES

An evaluation of the projects carried out at international or national level has not been made, but from the available public information on their effects we noticed a set of lessons learned that may be adopted in implementing a strategy to counter radicalization online, taking into account the objective of these projects and the way they were

[1] Within NCAZ as central authority there are BSI, BfV, and the Federal Office for the Protection of the Population and Disaster Support / BBK, as well as other authorities such as the Federal Office for Combating Crime/BKA, the Federal Intelligence Service/BND, Federal Police, Federal Army (and the Military Intelligence Service) and the Customs Investigation Office/ZKA.

disseminated. In our paper we took into consideration studies on security policy compliance (for example Bulgurcu et al, 2010;. Herath and Rao, 2009; D'Arcy et al, 2009;) that indicate that, in order to influence the security users' behavior one should change the way people perceive risks and make decisions related to security. To that end, as we presented above, some intelligence awareness programs go beyond simple communication of information related to security and are tailored taking into account cultural theory of risk, that is individual prejudices biases resulting from cultural and social values.

As we noticed, strategic discourse could be built on political or ideological considerations by different actors, who should take into account that social media discourses are more open, indefinite and give the public the possibility to participate and create new "elements" in the speech, which essentially are controlled by the author. In the cases presented a common strategy was to promote a single narrative disseminated through various media and supported by stand alone stories, which despite the fact that the public can change them, support the message as a whole, but are different from a classic strategic communication based on narrative and characterized by multiple actors distribution. These features are also visible when examining how Daesh uses social media to promote its discourse on "caliphate".

Taking these into account, in designing an alternative counter narrative one must take care to be a clear consensus on the strategy and purpose, meaning we need to answer the following questions:

- "who is the target audience?" - an individual, a defined group or mass public opinion?
- why we target that audience? We take into account vulnerability, risk or other variable?

Depending on the target audience, it is important to determine what influence the audience (emotions, reasons, combination of problems). This helps us to identify the reasons and therefore the content to be disseminated. Scale and scope will determine messengers, content and campaign assessment taking into account the following: a clear definition of the mandate; available budget and resources; the duration of the campaign and how it designed to be - reactionary in direct response to a recent incident or prolonged aimed at a slow change in public opinion.

Different messengers should be used for different types of narratives and they can work in a formal or informal type of cooperation. Cooperation is the best way to shape the broader context in which the campaign is to be developed. To that end, we identified five types of messengers that can promote our message:

1. Officials: government leaders, experts in communication and political advisors are best suited for promoting political and religious counter narrative;
2. Civil society and media representatives: members of civil society groups and journalists are considered credible for moral narratives. Families, social workers may also play a role in this field;
3. Religious, institutions and communities leaders: for countering religious narratives;
4. Former radicalized members: messengers may be appropriate to promote the message that there is nothing heroic about violent extremism;.
5. Victims: are considered to be credible messengers to determine the (potential) radicals to refrain from violence.

Credibility is as important as the message sent. Given that extremism is fueling itself from the feeling of distrust towards authorities, it is important to rely on third parties. "People like us" that connects online with "people who do not like us" is often as important as the existence of a group to send the message because it humanizes both sides offering alternative identity frameworks that promote the translation of the experiences of those who are not "us" for the target audience.

Dissemination channel must be chosen carefully according to the target audience and purpose. For example, an activity on a discussion forum needs months and has only a profound impact on an individual, while a counter narrative campaign can reach a much wider coverage of hundreds of users. Both traditional media (newspapers, radio or writing journalism) and new media (blogs, forums, discussion groups and video channels) can be used for dissemination.

Other method is to direct approach target persons to specific group events, for example, in schools. Messaging services like WhatsApp or Telegram can be used on a smaller scale. The websites tend to be information depositories and therefore provide more opportunities for interacting taking into account the following: they provide information, inspiration, and awareness; build social networks; offer workshops and media expertise.

Counter narrative time of delivery is determined by the project scope. If we are implementing a reactionary campaign, the best moment would be in the immediate aftermath of the incident. If we are developing a short to medium term campaign in response to a prolonged event, such as the Syrian conflict, the timing should be strategically planned for maximum impact. In order to do that we should have in mind the following questions: how often we have to produce content and how often should that content be updated or promoted using alerts? If we need a larger audience a good starting point would be to take into account some events considered to have impact, as for example local and school holidays and celebrations that can amplify the emotional impact. A successful online campaign is part of branding and advertising campaign, and therefore should effectively use all kind of manifestations of music, films or video production. Content and messages must remain "live" and relevant and to appeal to human emotions. However, we should avoid negative emotions, like fear, because they can dehumanize and strengthen extremist messages. On the other hand, humor can be a way to disseminate the counter narrative.

To create an effective model to counter jihadist narrative, one should have in mind extensive analysis that requires time and technical know-how to develop the guidelines that include interests and online communication ways to be used on the target group. Analyzing the studies on counter online communication, we identified the following types of alternative narrative that can be promoted:

- political narrative - disseminated by government leaders, counselors and communication policy that focus on combating the idea of "us" against "them";
- moral narrative - key members of civil society representative groups (including victims) families, social workers and colleagues who focus on immorality, murder and violence;
- religious narrative - religious leaders, institutions and communities that send the message that atrocities and crimes are against religious values;
- social narrative - former violent extremists who promote the idea that there is nothing heroic about violent extremism.

5. CONCLUSIONS

Security awareness program is designed to meet the different needs and attitudes of the participants. By identifying cultural biases and using them as a criterion for the identification and separation of target groups, we can improve program effectiveness without using significant additional resources, based on informed choices tailored to participants need.

Effective governance of online security is largely associated with security awareness programs whose purpose is to influence the users to comply with security policies. Security managers develop standards and best practices guidelines to plan and implement these programs. However, standards and guidelines adopt a normative-prescriptive approach assuming that the communication of security-related information will inevitably lead to compliance with security policy. Studies in various fields such as behavioral economics and health and safety, however, demonstrate that people interpret and internalize information about risk in terms of cognitive and cultural biases.

Beyond the economic and social benefits, opportunities to collect, store, and use data for illegal purposes will increase proportionally. Therefore, the capacity of all stakeholders to protect fundamental human rights and to respond effectively need to keep pace with these developments. From this perspective, any strategy to counter online radicalization should aim at creating an environment in which production as well as consumption of these kinds of materials not only become more difficult, from a technical perspective, but unacceptable, and less desirable.

The conflict participation of several actors along with opportunities that are created by information and communication technology development and democratization of technology have resulted in several of ethical and legal policy challenges, considerations and options. On the other hand, it seems that non-state actors can completely avoid legal issues regarding the use of social media, as long as they remain under the jurisdiction of civil liberal democracies and conditions of use set by the provider of social media.

BIBLIOGRAPHY

1. Atkinson, Robert D.& Castro, Daniel D.. (October 2008). *Digital Quality of Life:Understanding the Personal and Social Benefits of the Information Technology Revolution*. Washington, DC: The Information Technology and Innovation Foundation.
2. Weimann-Saks, A. Aly D. & Weimann, G.. (2014). Making “Noise” Online: An Analysis of the Say No to Terror Online Campaign. *Perspectives on Terrorism*. vol. 8, no. 5. 33–46
3. Bartlett, Jamie & Krasodomski-Jones, Alex. (2015). Online Anonymity, Islamic State and Surveillance. *Demos.* March.

4. D’Arcy, J.; Hovav, A. & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse. *Information Systems Research*. Vol.20, no.1. 79–98.
5. Sageman, M. (2004). *Understanding Terror Networks*. Philadelphia, PA: Pennsylvania University Press.
6. Neumann, Peter R. (2013). Options and Strategies for Countering Online Radicalization in the United States. *Studies in Conflict & Terrorism*. 36(6). 431-459.
7. Omand, D. (2015). *Understanding Digital Intelligence and the Norms That Might Govern It*. GCIG Paper No.8. Waterloo: CIGI and Chatham House.
8. Sisaneci I.; Akin O.; Karaman M. & Saglam.M. (20-21.09.2013). A Novel Concept For Cybersecurity: Institutional Cybersecurity. *6th International Conference on Information Security and Cryptology*. Turkey/Ankara