Preventing Terrorist Activities through Social Media

dr Aleksander Olech

25.06.2021

Main points:

- Security services cannot accurately monitor how much information both terrorists and radicalized people share online.
- Among the major social media platforms, a significant amount of content is posted under different subpages or channels. As such, there is a fundamental lacuna in nearly all research pertaining to harmful online content.
- Civil society serves the role of being the first and major anti-terrorist measure to inform and alarm law enforcement agencies.

Introduction

Along with others, the Internet and social media have provided terrorist groups access to two types of benefits. They entail the speeding up of communication amidst members of terrorist organizations or radicalized groups and offering said groups a chance to broadcast their attacks in real time.

Operating within clearly defined limits and a strict legal framework, citizens can be included in the government's holistic and comprehensive efforts to counter terrorism and extremism, following the narrative that every internet user can be a sensor. How can Europe's civil society be included in preventive online counter-terrorism measures?

The Internet as a Medium for Radicalization

A number of European nations struggle with an intra-state increase of online extremism and radicalization. Consequently, it is crucial to critically assess the issue of internet activity. There is an urgent need to verify possible threats to civil society and improve security measures for the benefit of citizens among European countries. Radicalization on social media platforms effectively leads to the destabilization of national integrity and threatens social security.[1][1] Such a situation is also essential for neighbouring countries and the international organizations that they belong to such as the European Union (EU) or the North Atlantic Treaty Organization (NATO).

[1] Ines von Behr, Anaïs Reding, Charlie Edwards and Luke Gribbon, "Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism" (RAND Study, Brussels, 2013), 6-8.

Due to the increasing number of far-right and far-left individuals as well as religious extremists - an international challenge, there is a need to improve national and transnational strategies that reach out for and maintain a high level of security. It must be stated that each country incorporates different measures to protect its citizens. However, one of the most crucial parts of every security system is the need for access to key information that has a significant meaning for the security of the state and could be used by terrorists.

Gaining access to critical information for maintaining security policies is less complicated than it may seem. Nowadays, most of an individual's life is strongly connected to their internet activity, where they share their privacy. Social media is full of photos, videos, geostatistic location points and phone numbers, personal views and comments, private thematic groups, and invitations to join particular organizations or events. Regardless, not all posts and shares are optimistic and directed to our close circle of friends and recipients. Some messages on social media are full of hatred, insults, rage, provocations and threats - many of which are strongly linked to terrorism. It should be highlighted that the Internet is a medium where terrorist activity has been developing.[2]

The Internet and social media have provided terrorist groups with two advantages. First, they both speed up and facilitate communication between members of terrorist organizations or radicalized groups, allowing them to easily coordinate global and regional attacks. Even more so, they grant such groups access to reach out to all internet and social media users with their tailored content. Second, social media has provided terrorists the opportunity to broadcast their attacks in real time and carry out long-term operations in cyberspace for instance as propaganda campaigns. The activities in the infosphere of terrorist cells, as well as far right and far left groups have shown that these organizations conduct not just single, independent actions but coordinate a series of them. These can be understood as a type of "infowar" in cyberspace that contributes to the spread of fear and uncertainty. Better said, they focus on intimidation aspects and increase their number of supporters, attracting recruits who are eager to arrive in the controlled areas to support extremist groups, or to conduct singlehanded terrorist acts as "lone wolves".[3]

[2] Mehmet F. Bastug, Aziz Douai and Davut Akca, "Exploring the "Demand Side" of Online Radicalization: Evidence from the Canadian Context," Studies in *Conflict & Terrorism* (2020), 43:7, 616-637, DOI: 10.1080/1057610X.2018.1494409.

[3] Ines von Behr, Anaïs Reding, Charlie Edwards and Luke Gribbon, "Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism" (RAND Study, Brussels, 2013), 15-21.

Awareness as an Initial Step towards Protection

The number of social media users that are registered on popular Internet sites grows daily. Undeniably, it is vital to take advantage of such an opportunity of global connection of people and use its global services for communication as well as a tool to inform individuals about security threats. More importantly, it could be utilized to educate civilians on how to recognize these threats along with radicalized persons. Citizens can also inform security services via special forms on websites managed by the police (as recently done in Austria and France). A procedure such as that significantly increases the number of people fighting terrorism, from a small group of trained counterterrorist officers to all a country's citizens, who can share their opinions and views through the Internet. Nonetheless, it should be taken into consideration that a downside could sometimes result from individuals' misuse of hotlines due to misinterpretations or other mistakes, which poses a strain to the resources of authorities. Despite that it is worth cooperating with citizens because the benefits may be higher than the losses.

The utilization of weapons by anti-terrorist troops cannot be expected to successfully and entirely fight terrorism and radicalization. A more comprehensive approach could include encouraging citizens to collaborate with authorities, which aims to ensure that society increases its efficiency. When a citizen informs the police of a threat, incident or attack, the cooperation is visible. This also applies to using social media as a means to track down possible terrorists or radicalized people. In this case, for example, they would get reported online, and the authorities will take action swiftly, significantly mitigating the time of response and allowing for pre-emptive action to be taken.

Evidently, security services cannot reliably measure how much material terrorists and radicalized people post online. For the major social media platforms, a substantial amount of content is posted under different subpages. A consequence of that is the existing fundamental lacuna in nearly all research about the sharing of harmful content online. To mitigate that, civil society serves as a first and major anti-terrorist measure to inform and alarm law enforcement agencies.

*This article was previously published by the Defence Horizon Journal: https://www.thedefencehorizon.org/post/preventing-terrorist-activities-through-social-media\\

ABOUT THE AUTHOR

Dr Aleksander Olech. Director of the European Security Programme at the Institute of New Europe. PhD in security studies. Specialist in the field of security and international relations. He gained research experience at the Université Jean Moulin III in Lyon, the Institute of International Relations in Prague, and the Institute of Peace Support and Conflict Management in Vienna. Scholarship holder of the OSCE & UNODA Peace and Security Program and the Casimir Pulaski Foundation. His main research interests are terrorism, international cooperation for security in Eastern Europe and the role of NATO and the EU with regards to hybrid threats.

IF YOU VALUE THE INSTITUTE OF NEW EUROPE'S WORK, BECOME ONE OF ITS DONORS!

Funds received will allow us to finance further publications. You can contribute by making donations to INE's bank account: 95 2530 0008 2090 1053 7214 0001

with the following payment title: „darowizna na cele statutowe"