CYPRUS CENTER FOR EUROPEAN AND INTERNATIONAL AFFAIRS
UNIVERSITY of NICOSIA

ISSN (online): 2547-8702

EASTERN MEDITERRANEAN POLICY NOTE

October 2025, No. 116

TERRORISM IN THE DIGITAL AGE

Isabelle-Yara Nassar

On August 19, 2014, the Islamic State frightened the world when they filmed the beheading of American journalist James Foley and posted it online. Kneeling in the Syrian desert, Foley was coerced into blaming the American government for his prolonged suffering and death before his head was cut off and displayed to the camera. The cruelty of his execution was intended to send a message to the West that their involvement in the region was not welcome.

Disturbingly, the video was not unprecedented. Footage from ten years prior showcased the similar fate of American journalist Nick Berg. The terrorist group responsible was exhibiting increasing extremity when they took Foley – who reported extensively on the Middle East for decades – hostage in 2012,[1] before establishing itself as the Islamic State of Iraq and Syria (ISIS) in 2013. The 2014 recording of Foley's death marked one of ISIS's first official acts, becoming one of the earliest examples of a militant group exploiting the internet as a weapon of terror. Traditional terrorism had entered the digital era.

Today, every geopolitical actor has formed an online presence, and terrorist organizations are no exception. The internet has no borders, making it an invaluable tool in an increasingly globalized world. Though governments and tech companies have taken measures to detect and remove harmful content, anyone can realistically post online. In today's age of simplified re-sharing, the rapidity at which content is spread – whether true or false – surpasses the speed of legal entities to act, making uploads effectively permanent. Non-state actors have leveraged this dynamic to advance propaganda and controversial ideologies across all available outlets.

Online platforms address two of terrorism's enduring challenges: geographical constraints and financial limitations. Though distinct, these obstacles are interconnected in regard to terrorism. Geography once confined acts of terror and member recruitment to the group's physical reach, and was financially compounded by travel costs, access to media, and weaponry. Border controls and intelligence services further restricted mobility, complicating attempts to reach a

Isabelle-Yara Nassar is M.A. student in International Development at SciencesPo Paris and Intern at the Cyprus Center for European and International Affairs (which is affiliated with the University of Nicosia).

wider audience. This was particularly true of groups operating in contested territories with limited freedom of movement.

The internet has largely eliminated these barriers by offering an alternative way to reach large numbers of people. Online platforms provide users with a low-cost, far-reaching medium for spreading propaganda and recruiting internationally. Even where fees exist, online dissemination is considerably more affordable than traditional communication channels, facilitating cheap and easy access to a wide audience. By democratizing access to mass audiences, the internet has disrupted the traditional media monopoly once held by states and private corporations. Consequently, people worldwide are now equally exposed and vulnerable to terrorist messaging and strategic propaganda. Historically, terrorists wreaked havoc on people in proximity to their activities; today, an event occurring thousands of kilometers away can terrify someone within seconds.

Undoubtedly, the internet has helped terrorist groups expand their reach; their potential audience online has become virtually limitless. Militant groups now spread their ideology and fear through various mediums in near real-time, undermining counterterrorism efforts. The reduced time needed to reach audiences enables prompt engagement and transnational radicalization.

This is further compounded by the creation of echo chambers - online environments where like-minded individuals cluster and share their beliefs. These spaces can be coded to prevent the infiltration of alternative viewpoints, reinforcing harmful ideologies and amplifying the concern. Echo chambers are often used by terrorists to engage, radicalize, and recruit new members who are receptive to extremist messaging. This heightened exposure is particularly concerning among younger demographics, whose belief systems are often still forming. Their constant online presence makes them especially susceptible to the psychological impacts of extreme content.

The radicalization of youth has become a clear national security threat, even in nations historically uninvolved in terrorism, such as the Netherlands.[2] Intelligence services and organizations worldwide - including the United Nations[3], the EU[4], and NATO[5] - have counterterrorism task forces that now include divisions for monitoring online content, underscoring the seriousness of this threat. This trend highlights a considerable rise in transnational radicalization, foreign terrorist fighters - individuals who leave their home countries to join terrorist groups abroad - and proxy attacks in locations far from a militant group’s base of operations.

For example, in February 2025, a 23-year old male radicalized on TikTok, carried out a knife attack in Villach, Austria, killing one teenager and injuring five others.[6] The incident occurred only days after a driver, found to have a similar motivation, drove a truck into a crowd in Munich and injured dozens of people.[7] Unfortunately, neither event was isolated, but rather was part of a growing pattern of online-coordinated violence. Digital forums now enable swift proxy operations: when a member from the originating location cannot travel, they can recruit and coordinate with someone abroad to execute an attack.

Research indicates that terrorist use of the internet continues to grow despite state-sponsored efforts to curb it. One of the most active platforms is X (formerly Twitter), which capitalizes on low levels of international regulation. A 2015 'ISIS Twitter Census' by the Brookings Institution estimated that over 46,000 Twitter accounts were linked either to group members or supporters, while highlighting a large increase of year-on-year account creation. These accounts, though mostly in Arabic and English, were found in multiple languages and across several continents.[8] A later 2017 Cornell University study by Baddaway and Ferrara analyzed millions of related tweets to understand online radicalization tactics. They found a heavy focus on islamic theology, violence, and sectarianism in ISIS messaging, and showed that online content often mirrored or anticipated real-world events, amplifying its perceived reach and power.[9]

Despite significant progress in counterterrorism capabilities, both legal systems and tech companies still struggle to evolve as quickly as the internet, putting malicious actors at a terrifying advantage. Although these platforms are becoming more sophisticated at filtering extremist material before it is shared indiscriminately, there is still a high risk of content getting through. The resulting transnational radicalization, youth recruitment, and proxy terrorism facilitated by online coordination remain major security threats. Given the rapidity of communication, this threat is likely to persist for the foreseeable future. It remains to be seen what advancements will be produced to counter this risk. No technology currently exists that has yet been bulletproof, so to speak.

Bibliography:

1. Callimachi, R. (2014, October 26). *The Horror Before the Beheadings*. The New York Times - Breaking News, US News, World News and Videos. https://www.nytimes.com/2014/10/26/world/middleeast/horror-before-the-beheadings-what-isis-hostages-endured-in-syria.html
2. *NCTV: Rising number of young people radicalised online*. (2025, June 17). National Coordinator for Security and Counterterrorism. https://english.nctv.nl/topics/terrorist-threat-assessment-netherlands/news/2025/06/17/nctv-rising-number-of-young-people-radicalised-online
3. United Nations Office of Counter Terrorism. https://www.un.org/counterterrorism/
4. European External Action Service. https://www.eeas.europa.eu/eeas/counter-terrorism_en
5. NATO. (2025, August 6). *Countering terrorism*. https://www.nato.int/cps/en/natohq/topics_77646.htm
6. Murphey, F. (2025, February 17). *Austrian knife attack suspect was radicalised on TikTok, officials say*. Reuters. https://www.reuters.com/world/europe/austrian-knife-attack-suspect-was-radicalised-tiktok-officials-say-2025-02-17/
7. Poltz, J., Rattay, W., & Guder, A. (2025, February 14). *Dozens hurt in suspected car ramming attack in Munich before German election*. Reuters. https://www.reuters.com/world/europe/several-injured-after-car-drives-into-people-munich-bild-reports-2025-02-13/

8. Berger, J. M., & Morgan, J. (2016, July 28). *The ISIS Twitter census: Defining and describing the population of ISIS supporters on Twitter*. Brookings. https://www.brookings.edu/articles/the-isis-twitter-census-defining-and-describing-the-population-of-isis-supporters-on-twitter/
9. Badawy, A., & Ferrara, E. (2017, February 8). *The rise of jihadist propaganda on social networks*. https://arxiv.org/abs/1702.02263