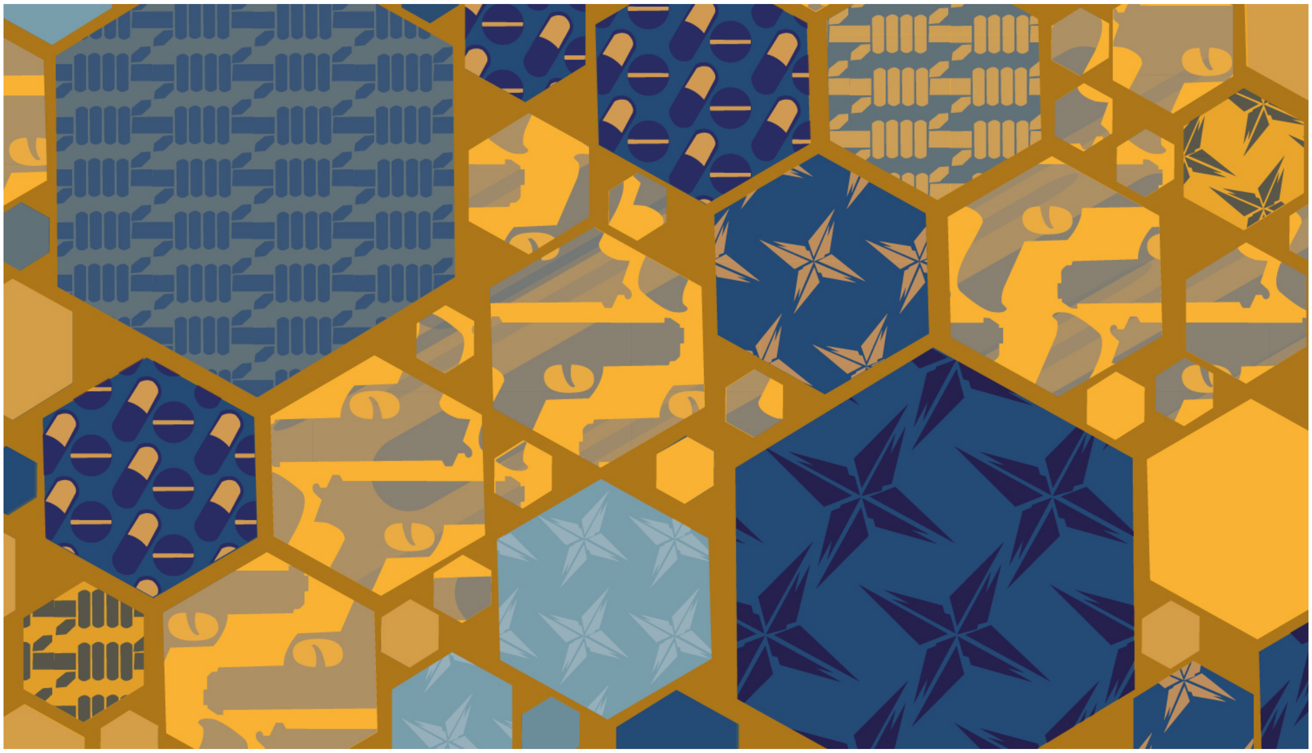
NATO Foundation
Defense College



CONFRONTING CRIMINAL/TERRORIST THREATS
The Reshaping of Non-State Actors

Policy Background Paper

Federica Lollo

NATO Defense College Foundation Paper

The 27th of October, President Donald Trump proudly announced the death of Abu Bakr al-Baghdadi, leader of the Islamic State of Iraq and the Levant (ISIL). He killed himself during a raid in the Barisha village (Idlib Province, north-western Syria, near the Turkish border) by elements of the 75th Ranger Regiment and the Delta Force.

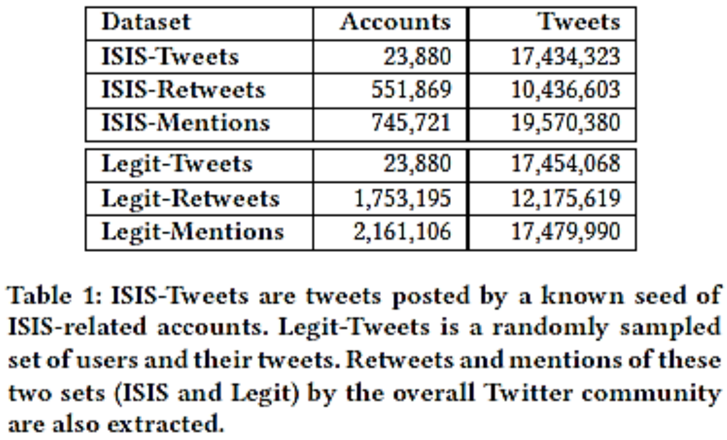
As in other cases, the death of a chief does not mean the end of an organisation. DAESH immediately designed as his successor the emir Abu Ibrahim al-Hashimi al-Qurayshi and, according to the Defense Intelligence Agency, the group is regaining foothold in Syria as a consequence of the US troops withdrawal. In the past, even the territorial defeat did not prejudice the survival of the organisation, which worked out new ways of acting and being funded.

In order to successfully neutralise these entities, it is important to dismantle the brand new social and cultural substratum supporting the construction of a multitude of terrorist organisations and groups in the region and abroad. While at the beginning this terrorism pretended to be based on religion, now more mundane (and Western) values seem to drive its recruitment (like revenge, self-empowerment, power, money and reputation)

The employment of Western technologies to jihadism includes the massive use of social media channels to convey propagandistic messages and the adoption of business criminal models that involve illegal activities at the core of their funding. These funds fuel terrorist attacks around the world and counterterrorism should take into consideration also these aspects.

Terrorists and extremists have been using the Internet to create relatively safe and anonymous havens to plan their future movements. Different reports illustrate what terrorists and criminals are doing to take advantage of the Net: hiding, recruiting, sharing their beliefs through propaganda, and fundraising.

In particular, over the past years, social media platforms have been at the core of ISIL propaganda activities. In the analysis *Measuring the Impact of ISIS Social Media Strategy*[1] is showed the interaction among ISIS Twitter accounts and the accounts of other Twitter users. The table below, comparing ISIS activities with those of normal random users, in 2015, highlights how deeply the group was penetrating the social media community:



Dataset	Accounts	Tweets
ISIS-Tweets	23,880	17,434,323
ISIS-Retweets	551,869	10,436,603
ISIS-Mentions	745,721	19,570,380
Legit-Tweets	23,880	17,454,068
Legit-Retweets	1,753,195	12,175,619
Legit-Mentions	2,161,106	17,479,990

Table 1: ISIS-Tweets are tweets posted by a known seed of ISIS-related accounts. Legit-Tweets is a randomly sampled set of users and their tweets. Retweets and mentions of these two sets (ISIS and Legit) by the overall Twitter community are also extracted.

In the first six months of 2016, Twitter suspended 235.000 accounts suspect of promoting terrorism. From then, online platforms have been trying to share their contacts database and to regulate their users' contents avoiding as much as possible to jeopardize their privacy and freedom of expression.

In September 2019, Facebook announced it would enlarge its definition of terrorist organisations and would deploy more artificial intelligence tools to improve the detection of posts that might be in some ways related to terrorism. One and a half year ago, Telegram started collaboration with Europol to counter online terrorist activities asking its own users to spot inappropriate contents.

[1] *Measuring the Impact of ISIS Social Media Strategy*, Majid Alfifi, Parisa Kaghazgaran, James Caverlee and Fred Morstatter, MIS2, 2018, Marina Del Rey, CA, USA. MIS2 is the workshop *Misinformation and Misbehavior Mining on the Web*; it was held in conjunction with WSDM 2018, Feb 9, 2018 - Los Angeles, California, USA, 2018.

As mentioned, social media promotion of terrorism also passes through illicit financing activities. From the paper *Social Media and Terrorist Financing. What are the Vulnerabilities and How Could Public and Private Sectors Collaborate Better?*[2] it emerges that terrorists use social media to finance their activities in three ways:

- The solicitation of donations on content-hosting services, mostly applying traditional payment methods such as banks;
- The communications through encrypted services;
- The misuse of crowdfunding online services under the labels of humanitarian causes.

All these elements prove that social media analysis may provide a valuable overview of the terrorist groups' activities and could represent a valuable tool to implement strategies against terrorism.

However, despite the increase of the virtual dimension of counterterrorism operations, counterterrorism on the ground remains a pillar in the hard security domain. Both the EU and NATO member states and partners have decided to collaborate against terrorism working within the framework of the *UN Global Counter-Terrorism Strategy* (adopted in September 2006 and reviewed every 2 years). At present, it is the only instrument available for the international community to enhance its multilateral efforts in the field.

Yet, the complexity of the current socio-geopolitical environment spawns new variables to consider in the implementation of counterterrorism strategies in order to guarantee security in its wider sense - for example, securing human rights to health, religion and freedom of expression. Indeed, the ambiguity in the definition attempts of "terrorism", often found in national legislation and entailed tools to combat it, leaves a conceptual, political and legislative vacuum that some governments may exploit for their own repressive policies.

[2] *Social Media and Terrorist Financing. What are the Vulnerabilities and How Could Public and Private Sectors Collaborate Better?*, Tom Keatinge and Florence Keen, Global Research Network on Terrorism and Technology: Paper No. 10, Royal United Services Institute for Defence and Security Studies, 2019.

Federica Lollo is Programme Manager at the NATO Defense College Foundation since 2016. She started her career working in different international bodies such as the International Organisation of the Francophonie and the United Nations Institute for Training and Research in the Multilateral Diplomacy Programme. In 2018 she collaborated to the volume "I Balcani occidentali al bivio. La NATO, KFOR e il ruolo dell'Italia", edited by Informazioni della Difesa, the official magazine of the General Staff of Defense, with the article "The Organised Crime in the Balkans."

NATO Foundation
Defense College