Radicalisation Awareness Network

RAN

Webpage: ec.europa.eu/ran

twitter | facebook | linkedin | youtube

08/03/2021

CONCLUSION PAPER

RAN small-scale event – Digital lone actors
24 February 2021 15.00–18.00 CET, online

Digital Terrorist and 'Lone Actors'

Key outcomes

How to find and identify digital terrorist "lone actors" before they commit violent acts was the lead question of this expert meeting. A special focus was put on the role and functions of social media platforms and gaming platforms. The term "lone-actor terrorism" has over time developed into a controversial and confusing concept. While individuals might act alone on an operational level, usually they are or feel as being a part of a specific group or movement. Particularly in the digital age, so-called "lone actors" usually are and feel neither lonely nor alone. Some "lone-actor" attackers did not join any group since they thought they would be under government surveillance, but they felt part of a collective united by shared values, actions and enemies. The trial of the Halle attacker (2020) and the Christchurch commission report (2020) indicated that neither intelligence services nor law enforcement nor the tech industry knew where to look for these digital lone actors or how to identify them online. Also, there was little awareness of the basic functionality (and abuse) of platforms, websites and other online services used by the perpetrators beyond Facebook, YouTube and Twitter.

Some of the key findings of the meeting are:

- So-called lone actors usually neither are nor feel lonely or alone. The narrative of the "lone wolf" is inaccurate and potentially harmful since it underestimates the milieus and informal networks that provide ideological, moral and sometimes logistical support to attackers.

- Look out for particular warning signs that could have indicate that an individual is moving towards violent action, such as starting to post hate speech or manifestos describing an existential threat to their in-group and justifying or calling for violence; sharing or actively seeking do-it-yourself instructions about weapons; expressing a "need to act"; ending relationships with individuals they claim are inferior due to their skin colour, beliefs, gender or other attributes.

- Funding for policy-oriented (short-term) research as well as for projects that focus on the digital (sub) milieus where potential digital lone actors might be active is needed.

This paper will first describe what challenges have been discussed from different perspectives shared. In the second part, recommendations for both practitioners and policymakers are presented.

Highlights of the discussion

The following challenges have been presented by experts on the topic.

- **Lone actors are not alone:** So-called lone actors usually neither are nor feel lonely or alone. The narrative of the lone wolf is inaccurate and potentially harmful since it underestimates the milieus and informal networks that provide ideological, moral and sometimes logistical support to attackers. Several cases of perpetrators who had been labelled lone actor/wolf turned out to actually be part of a movement or unorganised collective. A misinterpretation of the phenomenon can lead to a misunderstanding of the size and scope of the threat.

- **“Gamification” is not a new phenomenon:** The role of gamification in the context of lone-actor terrorism is potentially overrated, since the psychological framework of promoting status and rewards through competition is a common practice in (extremist/terrorist) groups. So far, there is no scientific evidence linking online gaming (including so-called first-person shooter games) to physical violence or extremist/terrorist behaviour.

- **Lack of governance on gaming platforms creates space for extremists:** Some gaming platforms/forums serve as meeting places, propaganda outlets and recruitment grounds for extremists or terrorists. Most of those services don’t have effective governance and moderation systems in place, which makes them easy targets for extremist and terrorist actors and for reaching out to specific audiences.

- **Room for improvement for social media companies:** Big social media platforms highlight that they invest significant resources in content moderation tools and procedures but claim that due to concerns regarding freedom of opinion and due to the amount of data, effectiveness will remain limited. At the same time, all user data is constantly being processed and analysed to serve the overall platform business model, which is to sell access to user profiles to third parties for advertisements. This indicates that social media companies could “know” more (or find out) about extremist or terrorist actors abusing their services than they do right now.

- **Can violent behaviour be predicted?** The question of which online behaviour could signal or indicate future violent action by individuals who express extremist behaviour online compared to those who are only “pretending” was discussed from different angles:

    - “Leaking” – Many lone actors have announced their actions before to family and friends or on specific social media platforms or websites. What is needed to process such information faster?

    - Risk assessment tools – The usefulness of risk assessment tools designed to mostly work with already known individuals like VERA-2R, TRAP-18, ERG22+ and RADAR-iTE for the identification of “unknown” digital lone actors should be explored further.

    - Learning from self-harm assessment tools (psychiatric experiences) – Experiences from self-harm assessment tools might be useful to identify potentially violent behaviour early on. This does not imply that lone actors necessarily have mental health issues and if they have them, that those are causally related to their terrorist actions.

    - Breakdown of protective factors – The online world can help “lone actors” to establish digital social bonds holding them in an emotionally safe space. A sense of urgency to act may come following a breakdown of protective factors or through apocalyptic narratives that promote an existential threat (e.g. “great replacement”/”white genozide”/”war against Muslims”) motivating the individual to change from victim to perpetrator or perceived “Hero”.

- **Overload of information:** Differentiating between noise and relevant signals is an increasing challenge, since the extremist digital landscapes are diversifying and the role of organisations is less dominant, especially in the violent right-wing extremism field compared to Islamist extremism and terrorism.

- **Changing digital landscapes:** As a result of the deplatforming of extremist/terrorist content from the big social media platforms, the digital landscapes are constantly changing. Extremist/terrorist actors are often moving to and between smaller social media and video sharing platforms or messenger services like Telegram and Chan boards. Those digital services are often less understood by prevention and countering of violent extremism practitioners.

- **Specialised support:** Many P/CVE practitioners who are active online might lack an in-depth understanding of the various (potentially) extremist subcultures, their usage of language, humour, memes and other kinds of "tribal signalling". Specialised CSOs can provide the insights necessary for analyses and digital outreach (e.g. for Digital Streetwork).

Recommendations

For practitioners, these recommendations are:

- When working with individuals, or the families of individuals, that have been labelled as lone actors, **make sure you investigate and understand their (online) social environment** and peers to avoid misjudging their motivations, values and support structure. **Learn from debriefings, trials and research** on what to look for to make sure you get the full picture. Ideally, certain practitioners (credible sources) need to be able to **engage in conversations**.

- Make sure you **understand the relevant and current trends, topics, memes, insignia and brands of the extremist (online) milieus** you are engaging with by reaching out to specialised civil society organisations and researchers who have the relevant expertise and experience. It is important to train practitioners, such as police officers and youth workers, to understand the specific humour and language online.

- Look out for **particular warning signs** that could have indicate that an individual is moving towards violent action, such as:
  - starting to post hate speech and manifestos describing an existential threat to their in-group and justifying or calling for violence;
  - sharing or actively seeking do-it-yourself instructions about weapons;
  - expressing a "need to act";
  - ending relationships with individuals they claim are inferior due to their skin colour, beliefs, gender or other attributes.

To identify digital signals of potential lone actors, **check** if existing **risk assessment tools** like VERA-2R, TRAP-18, ERG22+ or RADAR-iTE might be instructive or can be modified. For policymakers, recommendations are to:

- **Make sure digital extremist/terrorist milieus and movements that might guide and motivate a lone actor are appreciated and understood properly.** A misunderstanding of the lone-actor attacks as disconnected and isolated actions of individuals can lead to misleading statistics and incomplete threat assessments.

- **Prioritise funding for policy-oriented (short-term) research** as well as projects that focus on the identification of digital (sub) milieus where potential digital "lone actors" might be active i.e. mapping of actors to understand international connections, look at conversations across different platforms to potentially identify "lone actors", and to understand which prominent narratives are significant and relevant to these online actors. Research can be done in an anonymized format to identify trends and conversations across platforms.

- **Keep up the dialogue with, and pressure on, social media, video sharing and online gaming companies** regarding their efforts to not only deplatform terrorist content but also identify potential digital lone-actor terrorists in a proactive way. Online platforms and researchers should develop indicators to predict behaviour, including hate speech signals and see how they interact with other indicators, and to study patterns of behaviour over time, i.e. if there is an escalation of behaviours to identify lone actors through these behaviours.

Invest in structured and ongoing **peer learning modules** that facilitate the exchange of lessons learned between relevant actors (CSOs/researchers/government/companies).

Relevant practices

Some practices have been presented:

The 1-2-1 online interventions from the Institute for Strategic Dialogue is an experimental approach designed to fill the gap of not having systematised attempts to supplement counter-speech efforts with direct online messaging and engagement at scale. Delivered on Facebook to date and working across extreme right and Islamist ideologies, the programme provides an opportunity for individuals showing clear signs of radicalisation to meet and engage with someone who can support their exit from hate.

The Redirect Method by MoonshotCVE implemented by Facebook and Google can serve as inspiration. The method is designed to combat violent extremism and dangerous organisations by redirecting users who have entered hate- or violence-related search queries, towards educational resources and outreach groups. A pilot of the programme was launched with delivery partners Life After Hate in May 2019 in the United States and with Exit Australia in September 2019.

The project "Good Gaming - Well Played Democracy" by the Amadeo-Antonio Foundation in Germany combines analysis of gaming subcultures from a P/CVE perspective with digital streetwork by reaching out to online gamers and to educate them about harmful conspiracy myths. The project also trains teachers, social workers and influencers on those topics.

Follow-up

A structured and continued exchange between experts who work on digital lone actors' milieus and EXIT workers, who are experienced in online interventions, could generate additional practical insights on how to understand, prevent or counter this developing and changing phenomenon. A cross-cutting event on 'Lone actors – jointly taking stock of recent developments and combining knowledge' and a webinar on 'Digital Terrorist/Lone Actors' will serve as a follow-up on this meeting and stimulate further awareness-raising on the topic.

Product of the Radicalisation Awareness Network **(RAN)**,
Based on a paper prepared by **Alexander Ritzmann** and **Annelies Jansen**, RAN Practitioners Staff.