

17/05/2021

CONCLUSION PAPER

RAN Cross-cutting thematic event – Lone actors jointly taking stock of recent developments and combining knowledge

21-22 April 2021, online

Lone actors – Jointly taking stock of recent developments and combining knowledge

Key outcomes

In light of recent events such as the Christchurch attack, the Hanau shooting and the beheading of the teacher Samuel Paty near Paris, the threat of lone-actor violent extremism has grown within and outside the EU. While the topic has already been discussed in several RAN events and papers, activities of lone-actor violent extremists are constantly changing – also due to an ever-evolving digital landscape – and therefore underline the need to identify recent trends with different experts and preventing and countering violent extremism (P/CVE) stakeholders.

The objective of the cross-cutting event was to bring together researchers, policymakers and practitioners on the topic of lone-actor terrorism. While the topic is not new, the ways that we can identify and prevent such attacks are evolving, with the age of the internet, with increasingly better understanding of the mental health aspects of individuals at risk, and by building relationships and trust amongst different sectors: intelligence, police, mental health professionals, educators, who must work together.

Important insights from the joint discussion included the following:

- Numbers of lone-actor offences related to violent right-wing extremism (VRWE) are growing. Most of the VRWE lone actors were part of loosely connected online communities, which makes it difficult to identify who amongst the many individuals participating in such communities could pose a threat.
- The term “lone actors” can be conceptually incomplete or misleading. While attacks may be operationally prepared or carried out alone, P/CVE approaches need to acknowledge that the majority of so-called lone actors were embedded within online groups and networks, which often function as a replacement for other social contacts. So, while they attack alone, they are in fact from a very social online community.
- There are distinct features of how lone actors are connected with each other: VRWE lone actors were more loosely and ideologically connected with peers, sympathisers and violent extremist groups, while Islamist-inspired lone actors were, most often, in closer and direct contact with organised networks for recruitment, guidance or operational support.
- As lone actors were active in digital platforms, there is a need to improve digital good governance and information sharing on online behaviours and threats, and increased cooperation between online platform providers and P/CVE practitioners on transferring good practices in prevention to online spaces is also needed.

- Individuals are no less susceptible to carrying out an attack than organised violent extremist or terrorist groups and it is important to adapt risk assessment tools to include appropriate behavioural risk indicators.
- There is a growing need to increase the operationalisation of risk assessment and management tools in multi-agency settings. Improving mutual collaboration, self-evaluation and learning amongst practitioners from different institutions and from civil society can improve the validity of structured professional judgements.
- Comorbidity of mental health issues and criminality was identified in a number of lone-actor cases. Yet, connecting lone actors' violent extremism in a linear way with mental disorders risks oversimplification and stigmatisation. The key is understanding that mental health is likely one of a number of issues impacting the individual, and not always the principal one. Strengthening preventive mental health culture, comprehensive care concepts, and a tailored case-by-case approach are key elements in effective intervention.

This paper summarises the key outcomes of the discussions and highlights recommendations that emerged. By outlining the findings of the three parallel breakout sessions (Lone Actors in Digital Environments, Mental Health and Lone Actor Terrorism, and Risk Assessment & Management), this paper will present lessons learned and recommendations expressed by practitioners, researchers and policymakers.

Highlights of the discussion

The following challenges and trends were discussed amongst experts.

Lone actors in the digital environment

While lone actors carried out the operational attack on their own in most cases, they are often embedded in well-connected online communities and networks. This has repeatedly raised the question if the term lone actors might be misleading — particularly as radicalised and extremist movements, which originated in the online sphere, are increasingly making their violent impact felt in the offline world as well as the virtual one. In the past couple of years, the impact of extremist movements that started to mobilise on social media platforms and other online fora has become more visible in (violent) street protests and has fuelled a growing number of extremist violent attacks (e.g. the so-called Querdenker, Incels and QAnon).

Over the past couple of years, right-wing extremist (RWE) lone actors were increasingly committing violent extremist and terrorist attacks. Violent right-wing extremist lone actors were often connected to online networks and communicated by visual means (e.g. memes, videos, social media posts) encouraging each other to step into action. This makes it difficult to distinguish between group actors and lone actors as well as between online users who push others towards extremist activities and those who follow instructions or imitate other extremists. Compared to violent Islamist extremist (IE) lone actors, violent right-wing extremist lone actors are more loosely connected with their peers, which makes identifying individuals who may pose a threat even more challenging ⁽¹⁾. In fact, recent attempts to review the genesis of and lessons learned from lone-actor attacks, like the [trial of the Halle attacker \(2020\)](#) or the [Christchurch commission report \(2020\)](#), have underlined the continued challenges faced by intelligence services, law enforcement, the tech industry and P/CVE frontline practitioners in identifying digital lone actors online or signalling their content.

One of these challenges is the increasing trend of gamified elements in extremist digital settings, which create low-threshold entry points for individuals sympathising with extremist scenes. Such spaces provide a platform for individuals who want to seek inspiration or gain justification for launching violent attacks. Increasing gamification

⁽¹⁾ Bouhana et al., 2018: [Background and Preparatory Behaviours of Right-Wing Extremist Lone Actors: A Comparative Study](#)

also leads to an entirely new terminology used within such settings, which makes it difficult for outsiders to monitor and understand the content.

The use of automated detection tools of at-risk users and online warning signs raises ethical concerns and widens the scope of the privacy–security dilemma regarding individual privacy questions and national security interests ⁽²⁾. As (early) detection of extremist online content becomes increasingly relevant, questions arise as to which government agencies or institutions should be allowed to use such monitoring tools, what authorities should be able to use monitoring tools and what legislation is in place to prevent abuse.

Mental health and lone-actor terrorism

Mental health conditions can function as a catalyst as well as an inhibitor when it comes to committing a terrorist attack. Understanding (self-)destructive behaviours, experiences of exclusion and traumatic experiences in life paths is crucial to grasp individual cases of lone-actor extremism and in order to find tailored ways to address them. However, radicalisation processes of lone-actor extremists are often a complicated mix of biographical, socioeconomic, psychological and many other factors. Mental health issues might therefore not be relevant for individuals' susceptibility to lone-actor extremism, but rather one (of several) explanatory factors for their vulnerability to radicalisation. Misdiagnosis of where the issue sits in the individual's range of problems as well as more basic misunderstanding of the nature of an individual's mental health state remains a large issue regarding lone-actor violent extremism.

Possibly due to the implied meaning of the term lone actor, personal environments of lone offenders do not receive sufficient attention in some cases. However, their social contacts often play crucial roles in their (de)radicalisation processes. Mental health professionals, law enforcement and first-line practitioners should be aware of lone actors' family relationships and other social contacts, online as well as offline.

As mentioned above, lone actors' backgrounds may include (early) traumatic experiences. Rehabilitation of lone-actor offenders should pay attention to complex needs that also reflect comorbidity of criminality and mental health disorders. Diagnosed mental health issues of lone actors are often related to disorders of conduct that include sensation seeking, anti-social attitudes and impulsivity. The interrelation of different drivers for lone-actor violent extremism (e.g. loss of community, increasing stress levels, authoritarian personality) is, however, still under-researched.

As the cohort of lone actors remains heterogeneous and often faces great obstacles to access psychosocial services, there is a need to promote more comprehensive, easily accessible care concepts such as safe/care houses. If mental health services are used exclusively in the framework of referral mechanisms, without case-by-case assessment, this may increase stigmatisation or even the risk of (re)offending. Psychosocial support needs to be informed by a "life course approach" that focusses on the trajectory of at-risk individuals. To assess thresholds for violent behaviour of at-risk individuals in a comprehensive manner, it is crucial that psychosocial support practitioners enquire into and understand the function and intent of lone actors' behaviour, for instance, for what specific reasons individuals resort to violent action or toxic discourse online. Only focusing on assessing selected mental health indicators, such as the presence or absence of traumatic experiences, may lead to incomplete assumptions. To prepare such conditions, considerable investment in terms of resources, personnel and methodology is needed to build a preventive mental health culture within responsible institutions. The goal would be that individuals can access mental health services of multi-professional cooperation between police and mental health professionals, to ensure that they can ask for help without being stigmatised.

⁽²⁾ Verhelst et al., 2018: [Machine Learning Against Terrorism: How Big Data Collection and Analysis Influences the Privacy-Security Dilemma](#)

Risk assessment and management: Identifying, analysing and preventing lone-actor violent extremism

Individuals are no less prone to carrying out an attack than organised violent extremist or terrorist groups. In order to explain why lone actors decided to act alone rather than with a group or failed to embed within group settings, practitioners have used risk assessment tools (e.g. Terrorist Radicalization Assessment Protocol (TRAP-18)) to look at potential underlying risk factors, such as lack of social competence or idiosyncratic belief systems. The TRAP-18 is a structured professional judgement instrument with which law enforcement and other involved actors can structure and manage data on a person of concern for terrorist activities. Postdictive studies ^(3,4) have validated a number of TRAP-18 proximal indicators (warning behaviours) and distal indicators (individual psychological factors) for lone-actor violent extremism. As described above, individual psychological factors (distal indicators) are in most cases not easily detected. Proximal indicators, which are associated with the mobilisation of an individual, range from last-resort behaviours, noticeable novel aggressions, and attack/pathway planning to leakages of intent, in the form of online messages or manifestos.

Differentiations are to be made between threat assessment and risk assessment. Threat assessment refers to the detection of intended violent extremist behaviour before it is committed without direct contact with the lone-actor perpetrator. Risk assessment describes a process that examines the probability that a specific violent extremist **event** will occur as well as the consequences of the occurrence of this event and how tolerable the consequences of such an event would be. In general, risk assessment within the correctional system is mainly informed by studies comparing violent extremist and terrorist offenders who return to terrorist behaviours and those who do not, in order to identify indicators associated with a higher risk. However, this pool of subjects is very limited as, in many cases, lone actors do not survive their attacks, so risk factors have to be identified from a relatively small group (and mainly from true positives). From a scientific perspective, this is not entirely satisfactory, and makes it difficult to subsequently identify a useful range of specific behaviours that can shape useful risk assessment tools. Further, the complexity of trying to work on these assessments if a researcher is not directly involved with authorities with appropriate clearances is quite encompassing. Researchers who are not already working with authorities will find it impossible to get access to privileged information, such as police files or assessments of cases, or to interview offenders directly, meaning that most studies on lone actors rely on open-source information in order to identify typologies and "typical" patterns of attack planning ⁽⁵⁾. However, media reports can lack detail and accuracy, which does not always make it an ideal data basis.

While studying true positive cases helps to identify vulnerabilities of lone-actor violent extremists, it does not provide insights into the behaviours corresponding with the mindset of intent to commit a lone-actor crime or what mobilises individuals to do so. Basing research on a limited pool of cases, all of whom have committed offences, immediately creates a bias in the data set as there are no comparable control groups that can be used as a comparison to understand what a variance from the "norm" does look like (and therefore what a risk assessment tool should focus on). This adds to the fact that the volume of cases is very limited, which can create a challenging environment to collect enough data to be able to develop risk assessment tools that are able to appropriately provide practitioners with the right tools to manage potential lone-actor cases. More qualitative research comparing true positives and true negatives is needed.

Lone actors often announce their intent to attack in their digital networks prior to striking, something that is referred to as "leakage". However, social media contacts or family and friends are in many cases unsure whether to take such threats seriously and feel guilty about reporting suspicious posts. It can also be difficult to tell when someone means what they say they are going to do. When a troubled or angry individual who is about to launch a lone-actor terrorist attack announces they are about to "do something" online, it might be indistinguishable from their usual

⁽³⁾ Challacombe & Lucas, 2019: [Postdicting violence with sovereign citizen actors: An exploratory test of the TRAP-18](#)

⁽⁴⁾ Meloy et al., 2019: [Some TRAP-18 indicators discriminate between terrorist attackers and other subjects of national security concern](#)

⁽⁵⁾ Schuurmann et al., 2017: [Lone Actor Terrorist Attack Planning and Preparation: A Data-Driven Analysis](#)

online behaviour and commentary. There is a need to raise awareness on the topic of leakage when it comes to lone-actor extremism.

Recommendations

Several recommendations for frontline practitioners, policymakers and researchers were discussed during the plenary session as well as in the thematic breakout groups.

Digital environments

- As discussed above, lone actors are often embedded in active digital communities, which in many cases replace their lack of social contacts in the offline world. This poses a challenge for law enforcement and platform providers, as simply removing individuals from these groups or shutting down such online communities might only push them towards more extreme places in the Deep Web or darknet and/or act as a trigger for a larger collapse that leads them to commit a violent act. **It is therefore important to understand the (psychological) function such online communities have for lone actors and to develop online P/CVE approaches.**
- IE groups and VRWE networks are spreading extremist narratives in order to mobilise and instigate lone-actor terrorism. Incoherent fragments of hateful and extremist ideologies can be picked up, warped and recited on online fora by individuals and fuel motivation to commit an extremist/terrorist attack. Prior to committing offences, some lone-actor terrorists shared manifestos describing their extremist thoughts. Picking up on these signals and identifying possible threats requires stronger collaboration and information exchange amongst a wide range of actors, including platform providers, security authorities, researchers and P/CVE first-line practitioners.
- **While the effectiveness of alternative narrative campaigns is often contested and their impact is hard to measure, the amount of extremist online content mobilising lone-actor offenders calls for elaborate responses.** Depending on the degree of radicalisation of individual online users, alternative narratives and redirecting individuals to safer online spaces can hinder efforts by extremist actors.

Mental health

- **Avoiding stigmatisation with regard to mental disorders**, such as antisocial personality disorders, schizophrenia and autism spectrum disorders, within the context of lone-actor violent extremism is important. Though the correlation between mental disorders and lone-actor terrorism does appear to be slightly increasing, it remains weak and it is crucial to remember that the overwhelming majority of individuals suffering from such mental health disorders show no link to radicalisation processes. Increased media reporting on certain lone-actor attacks or a narrow focus on using mental health markers as referral tools risks building an incorrect direct connection between mental disorders and lone-actor violent extremism.
- Traumatic life events and experiences of exclusion can play a role in radicalisation processes in the absence of other coping strategies. **It is therefore necessary to understand the underlying function the extremist behaviour and the belief in extremist ideology has for individual lone actors.** Paradoxical interventions during rehabilitation processes might help lone-actor offenders to (re)gain control over symptoms they are experiencing. While paradoxical interventions are based on a complex concept, the main idea is that clients are confronted with the very symptoms they seek to resolve. In the context of lone-actor offenders, it is important to identify the (emotional/psychological) functions violent behaviours and the belief in extremist ideologies have for the individual. This can, for example, mean that individuals experience an immense fear of failure and are therefore more open to believe in "black and white" or extremist ideologies based on their motivation to try to avoid failure at all costs. In paradoxical interventions, such clients would be asked to fail at something on purpose, based on the belief that most individuals' behaviours indicate a need/function (e.g. seeking attention from parents or other persons). By actively exposing the individual to their symptoms, there is a chance to help improve understanding of their needs and ultimately how to control these symptoms

- **Providing space for peer-to-peer exchange between mental health professionals**, but also with other relevant P/CVE stakeholders, is important to improve joint action plans in developing comprehensive care concepts.

Risk assessment and management

- **More training is needed regarding the use and implementation of structured professional judgement tools.** If they are embedded in multi-stakeholder collaborations, first-line practitioners, policymakers and researchers should be included in evaluating these tools.
- There is need to review and update risk management and assessment tools to a changing reality of digital lone actors and **improve operationalisation of such tools by frontline practitioners.** Tools further need to be **tailored to a respective social and contextual environment** to avoid being too broad and thus not operational.
- **More qualitative research on smaller samples of recent true positive cases of lone-actor violent extremism is needed** in order to better understand and prevent lone-actor offences. At the same time, we need to further look into what prevented cases might look like (e.g. individuals who are part of the cohort but were stopped prior to committing an attack or offenders who were handled with non-terrorist legislation).

Relevant practices

Digital environments

1. The project [Good Gaming – Well Played Democracy](#) by the Amadeu Antonio Foundation in Germany combines a digital street work approach with the analysis of gaming subcultures from a P/CVE perspective. Project partners work together with gamers and experts on the topic to better reach out to at-risk and already radicalised online gamers in order to provide spaces for education on racism and conspiracy myths.
2. The [Estonian Web Constable](#) model aims to provide a tool for online users to flag extremist content and hate speech online. Web Constables are police officers with accounts on different social media platforms, such as Facebook, where they try to solve conflicts and discuss (local) issues with users.
3. Developed by [Moonshot CVE](#) in partnership with tech companies, the Redirect Method is deployed via online social media platforms such as YouTube. Through detecting online engagement with high-risk extremist content, respective users are offered alternative messages (e.g. intervention services, video recommendations including alternative narratives).

Mental health

4. “Safety Houses” in the Netherlands bring together different stakeholders, such as local government representatives, health and social welfare actors, police and youth workers, to jointly discuss local cases. Such services ensure early access to psychosocial care for radicalising/radicalised individuals.
5. Trauma-informed prison and probation settings can improve cooperation between security services and mental health professionals across all phases of prevention of lone-actor extremism.

Risk assessment

6. Tools such as the TRAP-18 and VERA-2 (Violent Extremist Risk Assessment) remain the most frequently used tools for cooperative risk assessment and management, including for lone-actor terrorism. The key function of these tools/frameworks should be to improve a joint professional judgement between government agencies and P/CVE professionals.

Follow-up

The findings of this cross-cutting thematic event will directly feed into two other RAN events:

- A small-scale meeting on the phenomenon of lone-actor violent extremism will take place later this year. The meeting will focus on one of the core themes (digital environments, mental health aspects or risk assessment) of the cross-cutting thematic event.
- To follow up on a small-scale meeting in Q1, a webinar on lone actors will address the role of digital environments for lone-actor violent extremism and terrorism.

During the cross-cutting thematic event, several topics were discussed that require further research and cross-sectoral efforts between practice, policy and research:

- As mentioned above, attacks by RWE lone actors are increasing and therefore receive growing attention by practice and research, while the focus has widely been on IE lone actors in previous years. More comparative studies between RWE and IE lone-actor extremism are needed.
- The role of digital spaces regarding lone-actor violent extremism, and particularly their potential in mobilising individuals, should be looked at in greater detail. Additionally, the question of online threat assessment and the detection of early warning signs remains relevant, also when it comes to cooperation between P/CVE stakeholders and platform providers.
- During the plenary discussion, references were made to discuss ways on how to guide at-risk users to safer online spaces. To ensure understanding stays apace with changing online environments, providing P/CVE practitioners with better resources and training regarding digital literacy, gamified terminology and changing online spaces is crucial.
- Potential and challenges that come with selecting control groups when studying cases of lone-actor violent extremism should be discussed in future events.

Further reading

- CLAT final report (2016) [‘Lone-Actor Terrorism: Final Report’](#)
- PRIME summary report (2017) [‘Preventing, Interdicting and Mitigating Extremism: Summary Report’](#)
- RAN C&N meeting (2018) [A psychological and neuroscientific perspective on how extremist propaganda works and how to effectively counter it](#)
- RAN C&N (2020) [‘Extremists’ Use of Video Gaming – Strategies and Narratives’](#)
- RAN HEALTH (2017) [‘Risk assessment of lone actors’](#)
- RAN POL (2020) [‘Lone Actors, Police and P/CVE’](#)
- RAN POL (2020) [‘Day-to-Day Challenges of Violent Right-Wing Extremism for Police, and Possible Responses’](#)
- RAN POL and RAN C&N (2019) [‘Current and future narratives and strategies of far-right and Islamist extremism’](#)
- RAN small-scale meeting (2021) [Digital Terrorist and ‘Lone Actors’](#)