

## CONCLUSION PAPER

*RAN small-scale meeting*

*23 May 2024 WebEx*

# Navigating Lone Actor Violence: Understanding trends and prevention

## Key outcomes

In recent years, an increase in the number of attacks by lone actors can be seen. <sup>(1)</sup> Often, these lone actors were radicalised online, inspired by a multitude of beliefs lacking ideological coherence, and blend (personal) grievances to rationalise their violence. This new phenomenon of “incoherent belief systems, combined with a kind of personal grievance” <sup>(2)</sup> can be understood as composite extremism.

As a result of composite extremism, the boundaries between different extremist ideologies have become increasingly blurred, creating challenges for P/CVE.

Therefore, the objective of this small-scale meeting was to explore the phenomenon of composite extremism, how the online environment influences processes of radicalisation towards composite extremism and to obtain a comprehensive understanding on best practices for practitioners working on this topic. Below, are the key meeting outcomes.

- In this newer composite extremism some narratives, such as misogyny, antisemitism and hostility towards authorities are persistent across manifestations of radicalisation.
- Since individuals operate online with **relative anonymity**, the signs of radicalisation may be less obvious to practitioners compared to those part of a structured centralised extremist network. Therefore, close bystanders such as family, friends and colleagues can play an important role in initial detection of radicalisation.
- Instead of identifying individuals at risk based on the ideologies and narratives they adhere to, it can be more effective to look at **common radicalisation factors**. There are a wide variety of different ideologies, but the underlying factors for these processes often overlap, such as existential insecurity, loneliness and nihilism.
- **Provide updated training to potential bystanders**, to ensure that they continue to have the capability and motivation to intervene directly or make referrals to practitioner support services. As extremism has evolved, confidence, awareness, or skills may have reduced, so this requires continuous investment.

<sup>(1)</sup> Europol (2023). [European Union Terrorism Situation and Trend Report](#), Publications Office of the European Union, Luxembourg

<sup>(2)</sup> Daveed Gartenstein-Ross, Andrew Zammit, Emelie Chace-Donahue & Madison Urban (2023). Composite Violent Extremism: Conceptualizing attackers who increasingly challenge traditional categories of terrorism, studies in conflict & terrorism

## Highlights of the discussion

### The role of online platforms in composite extremism

Online platforms provide opportunities for extremists to build a community, rapidly disseminate propaganda, trade tactical material, orchestrate activism, and even announce and broadcast attacks. Similarly, these platforms offer an environment whereby curious or vulnerable (young) people can easily encounter a wide range of extremist ideologies and communities, ultimately facilitating the process of radicalisation. Having this low-key access, also makes it possible for individuals to engage with and alternate between different extremist movements and ideologies, or combine different narratives into their own blurred ideology. See below a short case description, showing this blurred ideology. <sup>(3)</sup>

- Father introduces him to Nazism as a child. Mother says he really became interested in Nazism in 2001.
- As an administrator of an English language Salafi-jihadist forum, he posts things like, “a successful lone-wolf attack, even when it kills 1 or 2 or 3 of the kuffar is BETTER THAN an [sic] UNSUCCESSFUL massive attack which also results in your own arrest”.
- Under a pseudonym, he asks jihadists on the forum to use firearms, explosives and propane tanks against targets such as police stations, post offices, Jewish schools and daycare centers, military facilities, train lines, bridges, cell phone towers and water plants.
- Repeatedly tells his brother he wants to die a “martyr and take others with him.”
- Friend claims that a white supremacist group called him and asked that the individual lead a Nazi movement.

As a result of the above, the threat is becoming increasingly hybridised: the boundaries between different ideologies, false narratives, conspiracy theories, targeted hate, harassment, and violent extremism are becoming more and more unclear.

Some narratives however, such as misogyny, antisemitism and hostility towards authorities are persistent across manifestations of radicalisation, in this newer composite extremism. These so-called bridging narratives allow for out-group hostility, without the need for in-group identity formation. Violence-inducing conspiracy theories invariably draw on one of these three main narratives, but without a clear overarching objective or call to action. To this extent, they can be seen as core foundations of extremism, and should be tackled whether or not violence is the stated strategy, or a terrorist group is the stated affiliation.

### What can make a person vulnerable to composite extremism?

During the meeting, the factors that can make an individual more vulnerable to the influence of online narratives and radicalisation towards composite extremism were discussed. It was however concluded that these factors do not differ very much from traditional radicalisation processes. Some factors that were discussed are:

- a search for identity and belonging and the need for meaningful relationships with significant others: online groups and platforms can remove feelings of loneliness;

<sup>(3)</sup> Alexander Meleagrou-Hitchens, Moustafa Ayad (2023): The age of incoherence? Understanding mixed and unclear ideology extremism

- social isolation and, a sense of alienation from society as a whole and ontological insecurity due to global crises such as COVID-19; online groups and platforms can offer an allegedly safe haven;
- mental health issues such as loneliness, depression or autism spectrum disorders contributing to a person's vulnerability to the influence of online extremist communities, however most radicalised persons do not have a pathology;
- feelings of nihilism and search for meaning: having the feeling that the world is falling apart and that there is nothing that you can do, which is fed by the sharing of articles and papers within online communities.

## Challenges for P/CVE

One of the key elements of composite extremism, is the absence of a greater goal or overarching objective, such as building a caliphate or ethno-state. This comes with a more individualised and decentralised nature of extremism, making it more challenging to detect signals at an early stage. Since individuals operate with relative anonymity, the signs of radicalisation may be less obvious to practitioners compared to those that are part of a structured centralised extremist network. Therefore, close bystanders such as family, friends and colleagues can play an important role in the initial detection of radicalisation.

### *The role of family members as bystanders*

It was stressed that most bystanders are aware of the personal grievances that can make an individual susceptible for composite extremism. Because of that, they would also be able to observe changes in behaviour at an early stage. However, one of the key challenges addressed here is that family bystanders sometimes have the tendency to refrain from sharing their concerns, due to feelings of shame and the fear of stigmatisation. Cases were discussed where, after family bystanders shared signs of radicalisation with officials, it was often challenging to keep the family bond intact.

The role of family members in controlling their children's online activity was also discussed. One way to do this is by using parental control apps that help parents monitor and ensure greater safety for youngsters in the digital world (e.g. BARK app). It was however concluded that full control of children's online activity is practically impossible.

### *Online bystanders*

Another group of bystanders that can report with a certain degree of anonymity are those that are part of the same online communities as individuals at risk or those that encounter extremist content by accident. One of the challenges here is that not all online platforms offer easy possibilities to report extremist content. Additionally, online bystanders are not always able to recognise the signs of violence, since extremist narratives within the online realm are often conveyed through memes and "humour" to evade censorship.

## Recommendations

- Identify individuals at risk by looking at **common radicalisation factors** instead of the ideologies and narratives they adhere to, which can be more effective. There are a wide variety of different ideologies, but the underlying factors for these processes often overlap, such as existential insecurity, loneliness and nihilism.
- Invest in **making practitioners familiar with the signs of radicalisation** and related mental health issues that pose higher risks. This can be done, for example, through the development of a typology of different kinds of lone actors with signs of vulnerability overlapping and how to work with them.
- Facilitate the **development of digital literacy** by obtaining a more comprehensive understanding of online platforms. Each platform has different codes of communication and slang style, which could identify potential signs of radicalisation, therefore practitioners should understand how individuals communicate in a certain platform.
- **Provide updated training to potential bystanders**, to ensure that they continue to have the capability and motivation to intervene directly or make referrals to practitioner support services. As extremism has evolved, confidence, awareness, or skills may have reduced, so this requires continuous investment.
- **Bridge the online-offline divide**, by training practitioners, such as exit workers, to actively engage online with vulnerable individuals. Through digital streetwork or other approaches, these online conversations can acquaint individuals with an alternative narrative that can provide an answer to their personal grievances and lead them to support services as and when needed.
- With the evolution to a post-ideological landscape, and less focus on groups, practitioners need to focus more than ever on building protection mechanisms against common vulnerability factors, with more upstream and primary prevention approaches. This can include **building media and digital literacy** among (young) individuals; and **enhancing resilience** against the search for meaning, loneliness, and apocalyptic thinking.

## Relevant practices

- GAMER (supported through the Civil Society Empowerment Program) trained 17 gamers as active bystanders, using behaviour change communication approaches such as inoculation theory and entertainment-education. They were trained to counter online radicalisation and stimulate further active bystandership among credible fellow gamers. When evaluated (against a control group), they found that repeated exposure to these interactions created self-awareness and the ability to resist psychological pressure, as well as showing less prejudice, outgroup bias, and violent intentions.
- Parents for Peace (US) have provided guidance, educational materials, and skill-building tools to bystanders to support loved one and get healthy treatment. They have taken 100+ cases, with a wide variety of extremist ideologies, and allowed family members to reach potentially radicalising lone actors in ways that other stakeholders are unable to.

## Further reading

---

- RAN Small-scale expert meeting (2021). [Lone Actors: Making use of needs and risk assessment tools in P/CVE](#)
- RAN C&N Conclusion paper (2022). [Digital frontrunners: Key Challenges and recommendations for online P/CVE work](#)
- RAN Cross-cutting event Conclusion Paper (2023). [Prevention of violent extremism: A shared responsibility between mental health care and the security domain', The Hague 28 November 2023](#)
- RAN Specialised Paper (2021). [Lone Actors in Digital Environments](#)
- RAN Specialised Paper (2021). [Lone Actors as a Challenge for P/CVE](#)