Conclusion Paper

Thematic Panel 5

“Lone Actors: Who Are They, What Is Their Modus Operandi, and How Are They Connected Online”

11 April 2025, Brussels

EU Knowledge Hub on Prevention of Radicalisation

European Commission

1. Introduction

Thematic Panel 5 hosted its first meeting entitled ***"Lone Actors: Who Are They, What Is Their Modus Operandi, and How Are They Connected Online"*** in Brussels. It counted with the attendance of 21 participants, made up by EU Member States policy makers, mental health professionals, practitioners, researchers and law enforcement officers from across Europe. Participants were chosen following a balanced representation of gender and Member States, as well as considering the expertise of applicants and its fit into the topic of the thematic panel. In this vein, it is foreseen to maintain the same participants in future meetings, bringing thus continuity to the debates in the different meetings, and avoiding duplications in the discussions.

Thematic Panel 5, as part of the **EU Knowledge Hub of Prevention of Radicalisation**, aims to **clarify the concept of "lone actors"** to enhance EU-level cooperation on the issue, expand and consolidate knowledge on related topics guided by **EU strategic orientations** on countering radicalisation, thereby **supporting actors** (e.g., policy makers and practitioners) in Member States and priority third countries in **developing strategies, policies, methods, and practice**s, with the knowledge **produced compiled into a final report** translated into multiple languages.

The first meeting of Thematic Panel 5, focused on "Lone Actors – Who Are They, What Is Their Modus Operandi, and How Are They Connected Online," examined definitions of "lone actors" across Member States and research, evaluating whether they operated independently or were linked to other actors and small groups. It explored their modus operandi, the role of the online world in their activities, and the processes of their recruitment into extremism and terrorism via digital platforms, deepening insights into these dynamics.

Thus, this opening session addressed key issues such as lone actor's profiles, patterns and inspiration through an interactive and collaborative dynamic. The following guiding questions were set for this meeting:

- Defining Lone Actors: Who Are They?
- Which is the Modus Operandi of Lone Actors?
- How Lone Actors Connect, Interact and Radicalise Online?

2. Lone actors: who are and what we know?

Lone-actor terrorism is a highly complex and evolving phenomenon characterized by significant diversity in individual profiles, making it challenging to define a universal set of characteristics. **Demographic features** offer limited predictive value. Their behaviours are constantly adapting, rendering current solutions potentially outdated over time. While some have conditions such as autism or are on the neurodivergent spectrum, these factors alone do not explain violent behaviour, although they may contribute to a state of vulnerability, especially if they are in unstructured or emotionally unstable environments. These vulnerabilities can be exploited by extremist movements that use highly crafted digital content to attract and manipulate susceptible individuals, offering them a narrative that gives them meaning, validation or belonging.

A key element is **leakage**, where individuals often share grievances, ideologies, or plans prior to action, indicating they are not entirely isolated. The interplay between consumed messages and identity construction is significant, with risk factors spanning beliefs, attitudes, intentions, and behaviours. Distinguishing between internal thoughts and externalized actions is essential, as radical expressions do not always lead to violence, but certain behaviours may signal progression towards it.

Mental health is never the sole driver but it's part of a broader, intricate picture involving trauma, unstable relationships, social exclusion, substance use, identity struggles, and ongoing stress, among others. These complex needs, rather than isolated psychological disorders, better explain the vulnerabilities of these individuals. Therefore, the most accurate analysis starts from recognising how a cascade of accumulated problems can lead to a critical situation. Mental health-related issues will be examined in more detail during the panel's second meeting.

Similarities exist with mass murderers, particularly in risk factors, though differences emerge in preparation and execution phases. The concept of a "**perfect storm**" explains how personal grievances, psychological distress, and external influences converge, often in young individuals with limited protective factors. For instance, seemingly benign interests, like chemical experimentation, can escalate into engagement with extremist content.

A crucial element in early risk detection lies in the analysis of **online behaviour patterns**. Documented cases have shown how digital activity—such as repeated searches related to explosive materials or frequent interaction with violent content—can reflect a developing intent. This activity highlights not only the accessibility of extremist material online, but also how certain individuals actively use the internet to prepare attacks and to find communities that normalize and reinforce their beliefs. In this context, structured threat assessment methodologies have been developed to help distinguish between general expressions of grievance and actual pathways toward violence. Linguistic indicators—such as dehumanizing language, military-style terminology, obsession with previous attackers, or the adoption of a "warrior mentality"—can provide valuable insights when evaluated alongside professional judgment. These tools are particularly relevant in the absence of concrete intelligence, offering a systematic approach to interpreting fragmented digital signals.

Considering breakout´s feedback, there is no single ***definition*** for ***"Lone Actor"*** phenomenon. Member States use the category "lone actor" as an operational term to determine the existence of relation between the offender and some group, but it is not included within their national legal frameworks. However, academic and security approaches to lone actors can be distinguished. On the one hand, from a security perspective, an operational approach of lone actors seems to be more suitable since it is labelled as those individuals that operate without organisational support and execute an act by themselves. On the other hand, there is a wide variety of very ideologically-focused academic definitions that raise several concerns on where are the boundaries to consider an offender a lone actor. In this line, the following key challenges difficulty to reach a general consensus:

1. The boundary in violent acts between being considered as terrorism or mass-murderer actions, when it comes to lone actors.
2. The determination of when an individual becomes a lone actor, whether they have carried out the act or from the moment they begin planning it.
3. The difficulty to determine when a lone actor is connected to a group through the online ecosystem, and the different levels of connection to a network/group that can be identified.
4. The latter also raises doubts in how to measure the degree of affiliation of a lone actor to a group when interacting with extremist propaganda online.
5. The role of ideology, as some cases seem to be strongly influenced by ideological considerations - i.e. incels-, while others do not appear to be influenced.

One of the solutions proposed was to find a "minimum definition" based on a set of common elements in the modus operandi of lone actors. In this vein, common ***patterns*** in lone actors' attacks can be summarised in four points:

- Previous consumption of online extremist propaganda
- Attacks are typically indiscriminate, which means that they normally do not make differentiations considering the characteristics of targets
- Individuals usually self-finance their attacks, often using bladed weapons
- There are several cases of lone actors who committing mass murderers in order to be shot by police, and thus indirectly committing suicide.

Regarding the ***connection of lone actors to broader networks***, there is a general agreement that individuals are not totally isolated, as lone actors are normally connected online to propaganda, material or extremist content. Passive consumption of propaganda may be considered as a form of social engagement during lone actors' radicalisation processes, in which more in-depth research would be beneficial. In the same vein, research on lone actors that do not officially belong to a group, but claim loyalty to an extremist organisation after committing an attack – i.e. previous cases in jihadism and far-right - is needed as well.

Considering the ***profile*** of lone actors, they are profoundly gender-biased, observing that most perpetrators are male. This pattern may be reflecting the broader ideological and cultural reinforcements of gender roles within extremist ideologies. However, it should not be underestimated the role of women in far-right and jihadist groups in which they serve as recruiters, but also have perpetrated some attacks alone.

Around 30% of lone actors' attacks had been copied and/or ***inspired*** by previous incidents, which reveals how common this pattern is. Nonetheless, another notable observation is that the 58% of related attacks tend to occur within the seven days after a first major attack, suggesting a surge in activity and influence immediately afterward. It also may be interesting to consider this pattern for helping in early detection.

3. Online dimension

The **online environment** plays a pivotal role in many radicalisation processes, serving as a space for engaging with attack-related content, avoiding detection by surveillance systems, learning methods, signalling intentions, or seeking validation. Although direct recruitment is

not common, attempts to recruit individuals with high levels of suffering are observed -e.g. through propaganda-, offering them a cause to join or a justification for their pain. In this environment, the construction of identity and purpose can be as powerful as any structured ideology.

As stood out in previous section**, minors** are those more vulnerable to ***engage*** in online ecosystems of radicalisation and becoming lone actors, noticing that they are becoming radicalised at a younger age. Internet ecosystems are constantly being shaped by the user's needs and interests, creating self-reinforcing ideological bubbles and echo-chambers. When dissenting voices are excluded and own beliefs reinforced, group polarisation is fostered, which refers to how radicalisation mechanisms are intensified online due to confirmation bias, internet cookies and algorithm-driven content reinforcement. In this sense, the amplification and escalation of radicalisation processes within these ecosystems can be understood through the virality of the content that a small number of users can rapidly spread to a wider audience.

However, there is an intense debate about whether a lone actor decides to act before entering the bubble or after entering in it. In this vein, the role that **an individual's interests and needs** play when engaging with extremist actors and online extremist environments is key to understanding how this process works. For instance, an individual may be interested in 3-D printing, and without preliminary intention, the individual can engage with extremist communities and be recruited by them through this shared interest. On the other side, the needs respond to the role of individual’s grievances such as isolation and rejection feelings have in leading individuals towards radicalisation. Along with a wide variety of grievances, mental health issues are also considered one of the key potential contributors to lone actor behaviour. Nevertheless, sensationalist narratives around radicalised people with mental health issues should be avoided, as well as the oversimplification that position mental illness as the only and main driver for violent extremism.

Video games and instant messaging platforms such as Telegram or Discord can also play a significant role in radicalisation processes, bridging young people to other Deep Web platforms where more extremist content is shared. In this vein, the presence of ***recruiters*** in video games can be remarked, where they look for and recruit vulnerable individuals. Additionally, extremists can retroactively identify individuals who have left traces of allegiance online, even without direct contact. One of the key challenges that can be pointed out is how to assess the seriousness of online extremist content, as it is sometimes portrayed as humour or jokes, but contains a strong ideological significance which is

attractive for engaging individuals. Extremist communication styles should therefore be analysed more in detail.

Super-spreaders, a broad category encompassing but not limited to ***influencers***, play a significant role in shaping violent beliefs by disseminating content that can radicalize audiences on mainstream platforms. While influencers themselves are not typically at high risk of radicalization and are often driven by financial gain rather than ideology, isolated cases like Andrew Tate demonstrate their potential to amplify radical narratives. Additionally, super-spreaders can blur the lines between conventional and radical discourse. In contrast, religious leaders may pose a more substantial risk, as their influence over followers can facilitate the spread of radical beliefs.

Finally, concerning the ***early detection*** of lone actors, there is a lack of systematic approach for detecting them, apart from the continuous monitoring of online content by law enforcement agencies. Thus, the lone actor phenomenon is highly unpredictable. In this line, finding a solution on how professionals in the field can inject alternative narratives into online extremist environments for disrupting the reinforcement cycles supposes one of the biggest challenges.

When it comes to legal tools, law enforcement agencies cannot monitor and control some aspects and/or individuals online if there is no legal reason that justify the intervention. In this vein, the use of criminal law as a preventive measure against violent behaviours may be dangerous and the last resort to use, as the protection of fundamental rights and freedoms should be ensured.

4. Key Outcomes and Identified Knowledge Gaps

First meeting of Thematic Panel 5 was focused on consolidating insights and identifying key priorities for the next stages of the Thematic Panel. The first panel gathered information on how the term "lone actors" is understood in different member states and contexts, and how lone actors operate in the online environment. The main outcomes of the meeting are:

- There is **no single definition of “lone actor”**. The term "lone actors" needs to be more clearly defined in order to enhance EU-level cooperation, national strategies and policies, as well as operational collaboration.

- **Leakage** —the prior manifestation of personal grievances, ideology or violent intentions— **was highlighted as a key element in the early detection of risk**.
- Mental health is not seen as a single casual factor, but as a part of a more complex picture that includes trauma, identity crisis, social exclusion or prolonged stress. The **role of grievances, isolation, and rejection** from society plays **a critical part in the radicalisation process**, especially among young individuals.
- The **digital environment** plays a key role in radicalisation processes, facilitating access to attack-related content, the acquisition of knowledge, evasion of monitoring and, in some cases, the search for validation or legitimacy. Online networks incite and encourage lone actors.
- **Lone actors are rarely entirely isolated**; they are often connected to extremist narratives or content through loose online networks, which can be as significant as, or more so than, direct affiliations with organized groups.
- Early detection of lone actors can be difficult, but those connected to groups or networks are more easily identifiable.

Additionally, several ***gaps*** were identified in current knowledge and practice:

- Participants highlighted the need for improved methodologies to differentiate between radical expressions and actual pathways to violence.
- The absence of a unified definition of "lone actor" complicates communication and collaboration across sectors.
- Current approaches were considered overly focused on ideology, sometimes overlooking psychological drivers or mixed motivations.
- The importance of continued research into passive online consumption as a form of social engagement was also noted, as well as the challenges in assessing the degree of online group affiliation.
- Discussions also stressed that there is rarely complete isolation—lone actors are frequently connected to extremist content or narratives, even if not directly linked to organisations.
- The presentations and discussions also revealed a paradox worth leveraging for prevention: while risk factors receive significant attention and extensive research, protective factors—despite being easier to implement—remain underexplored.

5. Next meeting

Looking ahead, the panel will focus on building knowledge to assist Member State stakeholders in developing policies, strategies and practices to prevent lone actor actions and potential attacks, including the development of practical guidelines and improved early detection mechanisms. These efforts will continue in the ***upcoming meetings*** in June (Helsinki), September/October (Dublin), and the final session in November/December (online), leading to the development of delivering a final report to support policy and practice across the EU.