

12/02/2021

CONCLUSIONS PAPER

RAN event – Small-scale Expert Session

16 December 2020 – online

Radicalised police, military and prison staff

Key outcomes

Radicalisation amongst military, police and prison staff is a hot topic within the prevention and countering of violent extremism (P/CVE) community as some incidents of members of such forces carrying out attacks or circulating extremist content have made headlines throughout Europe in the past years. However, the topic seems to be complicated to approach: due to its sensitiveness, it can be difficult to establish a full picture of the situation. What are the numbers, what are the different layers of the problem and how can we effectively counter it? And, more importantly, how can we create an awareness as well as neutral grounds for follow-up activities where all actors feel safe enough to share insights?

The RAN Small-scale Expert Session on the topic of “Radicalised police, military and prison staff” took place on 16 December 2020 and aimed at tackling these issues. The meeting gathered researchers as well as practitioner experts on this topic. The key outcomes of this meeting were the following:

1. There was a shared sense of urgency that the radicalisation of military, police and prison staff is a pressing phenomenon that has **not been explored enough**: the risk is that it could be underrated.
2. **Data are missing**, so it's difficult to have a clear picture of cases of radicalisation of prison staff, police and military.
3. The approach to the topic could benefit of the expertise and approach on **insider threats** in the context of critical infrastructure. Organisations may already have experiences with how to detect suspicious behaviour.
4. Organisations and employers have options to work on **creating an organisation that is resilient** to radicalisation, with, on the one hand, awareness, reporting and sanctioning, and, on the other, attention to a healthy working climate, professional standards and the safeguarding of staff against risks related to their job, radicalisation being one of these.

This paper will reflect the outcomes of the discussion and, firstly, focus on the highlights of the discussion, such as a first reflection on the reasons why individuals radicalise within the police, military and prison, and then summarise the recommendations that were formulated by the experts, such as for institutions to allow researchers access to data.

Highlights of the discussion

- **Image of security forces, law enforcement and prison staff:** The topic of radicalisation within these groups is extremely delicate and can strongly influence how an agency is perceived by the public and therefore also its legitimacy and acceptance amongst a country's citizens. It can be extremely difficult for agencies to communicate this topic when large parts of the information are confidential and cannot be published. Cases of radicalisation amongst those professionals can seriously hamper the credibility of the respective organisations, with negative impacts on their daily activities and on their credibility.
- When discussing this topic, it is important to keep in mind that there are **legitimate reasons** to join the military or law enforcement — it can be a rewarding career. For example, a certain degree of patriotism is not an indicator for possible radicalisation. However, some of these reasons, when “pushed” beyond certain limits, might lead to behaviours that have nothing to do with the mission of the concerned organisations, and might also feed into a potential ground for being radicalised and recruited.
- Why do individuals **who are already radicalised** join/try to join the military or law enforcement?
 - **Access to professional training:** While unauthorised access to weapons is highly unlikely, access to training with weapons can be a strong motive for already radicalised individuals to join the military or law enforcement. Some aim at increasing their fitness level or their ability to handle weapons that they can use in other contexts. This applies especially to right-wing extremists and individuals who are working towards the collapse of society and their respective government.
 - **Ideological component:** Especially in the right-wing extremist scene, being part of the military can increase an individual's credibility for the scene because it supports the notion of fighting for one's nation. In the last years we have seen an increased attempt by extremist organisations to recruit individuals who are/have been working in the military or law enforcement. This might be also a pull factor for already radicalised individuals to join.
- **Radicalisation amongst prison staff:** It is important to consider that processes of radicalisation amongst prison staff have many layers and can have a multitude of reasons. The environment where they work is peculiar: in the prison context, staff are confronted with sentenced criminals. An example can help to clarify how the prison context can have an impact on a radicalisation process: in some European countries the number of inmates coming from third countries is over proportionally high amongst prison populations. This can increase prejudices towards minorities living outside prison, and possibly be a push factor for right-wing radicalisation. Inmates could confront staff with hostility and sometimes even violence; this feeds susceptibility and can be a trigger event. On the other hand, in other EU countries (e.g. in eastern Europe) the percentage of the foreigners among the prison population is much lower than in other parts of Europe, and therefore the main drivers to right wing radicalisation will be different. Regional differences matter also when we explore the radicalisation in uniform.
- It can be interesting to look at adjacent fields such as **insider threats to critical infrastructure**, as some organisations may already have experiences with how to detect and prevent harmful behaviour within their organisation, and motives and processes of radicalisation may not differ that much from radicalisation of military, police and prison staff.

- These insider threats also **jeopardise the image of, trust in and effectiveness of** of state bodies. Extremists are at war with the system, with the state. The fact that state institutes are seen as corrupted by extremist elements will be exploited in the extremist propaganda (“You see, they are racist and Nazis”). Having extremist issues in the organisation can e.g. hamper the receptiveness of prisoners to disengagement, deradicalisation and rehabilitation; police might have more difficulty in being trusted by communities and receiving information.
- **Organisational culture:** One of the main challenges is to create an atmosphere in which staff are willing to report possible cases of radicalisation and extremism. In many cases, organisations are characterised by a strong feeling of togetherness and unity; reporting a colleague is not done.
- The Taxonomy of Espionage & Insider Threats, as was presented by Kenneth Lasoen, could offer a structured way of identifying the risks of radicalisation of staff that could lead to managerial responses.
- There is a risk that radicalisation “goes with the job”. On top of the recognised set of known push and pull factors for radicalisation, there are **context-specific job-related push and pull factors and trigger events**.
- There are several modus operandi: individual employees could radicalise **on their own**; staff could be **targeted from outside recruiters**; extremists could try to **infiltrate** by applying for a job to get inside; colleagues can **“peer/group radicalise”** in a toxic or permissive environment.

Recommendations

Practitioners and management level:

- **Do not assume that your organisation is free of extremism and the risk of personal radicalising.** One of the most important aspects to remember is that it can happen anywhere and to anybody.
- **Background checks are only a snapshot** in time that cannot give a long-term and sustainable picture of the development of a staff member and should not be relied on.
- **Provide training:** Military, police and prison staff need awareness training on radicalisation, detecting early signs of radicalisation amongst staff at work, and also with colleagues. The training is also related to training in professional ethical behaviour and attitudes.
- If **signs are downplayed** as jokes or a trait of character, processes of radicalisation can go unnoticed. Trainings should also include possible scenarios of radicalisation and how that can specifically harm the respective organisation.
- **Organisational culture and procedures:** Management needs to initiate an atmosphere of trust where staff feel enabled to report possible cases of radicalisation. The risk of over surveillance and of a perceived lack of trust exists. The internal communication strategy should highlight that reporting cases of radicalisation does not equal treason but rather the protection of institutions by strengthening their credibility, transparency and ultimately also legitimacy. More than reporting, it is also about safeguarding employees from the risk of radicalisation, and creating healthy working conditions. Staff who feel neglected and are struggling with conflicts or incidents at work are more at risk of risky behaviour.
- **Taxonomies**, such as the one presented below under “Relevant”, can help to assess the unique characteristics of the organisation and its staff. Personnel with grievances and a work conflict are at a heightened risk of radicalisation or being recruited.

- The need for **more data**: It is evident that practice as well as research is missing data. The official numbers of cases of radicalisation reported in military, police and prison staff are likely to be outnumbered by a “dark number” that is currently not being reported. This is of course due to the sensitive nature of the topic. However, without concrete data, prevention and intervention measures are difficult to plan and implement.

Researchers:

- **“Dark numbers”: data, researchers and Member States.** As of now, there is still a lack of data, which hinders a holistic analysis. This indicates that there is a need to include more academics and researchers in the discussion. There is a need for more explorative studies that require access to official data from and on military, police and prison staff.
- Apart the general push and pull factors for radicalisation that apply to all individuals, the context-specific job-related push and pull factors should be further explored.
- To get a better overview of the scope of the problem, there is a need for **further definitions** of insider threats as well as the different layers of radicalisation in military, police and prison staff. This can help to more easily detect and categorise cases.
- Researchers need to engage with practitioners, policymakers and the management level of institutions equally: It is a cross-cutting topic that requires a **multi-agency approach**, even during the exploratory phase.

Relevant

Kenneth Lasoen, lecturer in intelligence at **Antwerp University (Belgium)**, presented his taxonomy, which can help organisations to be aware of points that are related to the risks of a certain individual. The taxonomy can play a role in the assessment of new colleagues, but also in creating a healthy working climate preventing or countering these risks.

Taxonomy of espionage & Insider Threat

PREDISPOSITIONS	MOTIVE CATEGORIES	TRIGGERS	OBSERVABLES
<ul style="list-style-type: none"> • Mental health disorders • Personality problems • Challenged social skills and/or decision-making capacity • Problems with rules and authority • Addiction • Immaturity (fantasy-driven, insecure) • High intelligence (negative creativity) 	<ol style="list-style-type: none"> 1) power reassurance (compensatory) 2) power assertive (entitlement) 3) anger retaliatory 4) anger excitation 5) opportunistic 6) profit oriented 7) disaffection 	<ul style="list-style-type: none"> • Stressful events • Life crisis • Perceived slights or injustices • Denied promotion • Abusive supervision • Loss of position • Poor review • Financial difficulty • Sadistic pleasure • Thrill seeking • Deep-seated beliefs 	<ol style="list-style-type: none"> 1) Ideological or rationalizing pathway <i>identification and fixation, distancing and objectifying</i> 2) Personality change <i>observable stress, impulsivity, aggression, abnormal social contacts or isolation, disregard for rules</i> 3) Attack contemplation <i>makes ultimatums, aggression frequency, paranoia, expression of imperative</i> 4) Attack planning <i>Try-out behaviour, access anomalies, unusual presence, leakage, concealment efforts</i> 5) Attack preparation <i>Focused activities, deliberate manipulations or exploits</i>
<p>DARK TETRAD OF PERSONALITIES:</p> <ol style="list-style-type: none"> I. Machiavellianism II. Subclinical narcissism III. Subclinical psychopathology 	<ol style="list-style-type: none"> 1) Self-promotion/grandiosity 2) Low empathy 3) Duplicity/lack of integrity 4) Aggressiveness 5) Anti-social 		

Figure 1. Taxonomy of threats

© Kenneth Lasoen, Antwerp University

Follow-up

- There should be a higher number of events that bring together practitioner experts as well as researchers to together explore the data we have, and to enlarge the data set in order to elaborate on the scope of the issue.
- There is a need for more meetings under the Chatham House Rule in order to create a safe space for all relevant actors to share insights and, for example, numbers. This can help to lay a first basis for possible follow-up formats.

Further reading

While there is still a lack of data on cases of radicalisation in military, police and prison contexts, there is a variety of reports and lessons learned that tackle the topic, as well as from adjacent fields such as insider threats to critical infrastructure.

If you are interested in reading more about insider threats, the report of Matthew Bunn and Scott D. Sagan, [‘A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes’](#), includes recommendations that can also be transferred to the military, police and prison contexts, such as that background checks alone do not solve the problem.

Moreover, there are a number of country-based reports from the respective intelligence and security services that explore the topic, such as a [French report on the threat of radicalisation in public services](#) as well as a publication of the domestic intelligence service of the Federal Republic of Germany on [right-wing extremism within German security forces](#). Both reports are only available in French and German, respectively.