RAN POL

20/04/2021

CONCLUSION PAPER

RAN POL Preventing and countering radicalisation of police, military and prison staff
23-24 March 2022, online

Preventing and countering radicalisation of police, military and prison staff

Key outcomes

On 23 and 24 March 2022, a group of experts with experience in police, military and prisons gathered online to discuss preventing and countering of radicalisation within their organisations. With presentations and reflections, participants from different Member States shared their experiences and views on the topic.

Against the background of some well-known incidents, and some unknown cases, it was clear to all participants that no institution is immune to radicalisation of staff members or to other insider threats. Sometimes early and 'light' radicalisation is observed, but sometimes - unfortunately- we are confronted with deadly blue-on-blue attacks.

The distinction was made between PVE and CVE. On the one hand, on CVE, the discussion was about detecting, referring and sanctioning. On the other hand, participants talked about prevention (PVE) by discussing the question how to invest in a healthy organisation with high professional standards as a shield against extremism.

The following key outcomes were identified from this discussion:

- Ongoing vetting and screening of staff on insider threat and radicalisation is crucial, not only during the selection process but also systematically within the whole service.
- training and awareness-raising of staff and management on internal threats have to be constantly implemented.
- The Code of Ethics can put a bigger emphasis on keeping unwanted developments out, and can help boost high professional standards.
- Good leadership implies prevention and a healthy work culture/environment.
- There are concerns about the rising number of right-wing extremism within police, military and prison staff .

This paper summarises the main conclusions following presentations and group discussions during the meeting. During the meeting, this topic was discussed considering CVE and PVE. Therefore, the recommendations focus on detecting and countering radicalisation within the police, military and prison organisations. Additionally, the recommendations also point out how to prevent radicalisation within organisations by having adequate management/leadership and healthy work culture in the police, military and prisons. Having a healthy work environment and leadership that promotes this with openness will built resilient organisations and staff.

Highlights of the discussion

Insider threat and radicalisation

- Holding legitimate political views is not considered extremism. However, there is a problem if expressed or furthered by statements, deeds or actions which result in harassment, intimidation or threats of violence against individuals, society or institutions.
- An "insider threat" is a person who has access to critical infrastructure or sensitive information and who, through his/her position and knowledge, exploits the vulnerabilities of the infrastructure or the system or allows others to abuse them, thereby possibly having a major negative impact on the functioning of the organisation or the wider society.
    - The insider threat includes the threat of radicalisation, terrorism, espionage or domestic extremism.
    - An individual may have joined the organisation with existing extremist views or may have developed these views later. They may have been targeted by extremist groups because they are in the organisation or the extremist groups may have persuaded them to join for their own ends.
- Radicalisation and other non-professional behaviour is damaging the reputation of these crucial state institutions and will fuel anti-government sentiment and other extremist groups' views, opinions and beliefs. A damaged reputation threatens the effectiveness of organisations as well.
- Vetting procedures have proven insufficient if not done properly (in-depth) or regularly.
- Participants from police, prison and army from all over Europe reported that they were concerned about the growth of right-wing extremism among their colleagues.

Behaviour detection

- The detection of potential insider threats starts with behaviour detection of unfamiliar or worrying behaviour and attitudes.
- When people see unfamiliar behaviour, there is a threshold to refer/report. The detection process is characterised by questions and approaches:
    - Is there radicalisation or just innocuous behavior?
    - Colleagues think they are not allowed to report on their colleagues.
    - They do not want to "rat out" their colleagues or face group pressure.
    - The declarant is afraid of negative consequences.
- "Military mentality" risk playing an important role in the reception of extremist beliefs.
- There was also an important conclusion on the need for support and assistance for the officers at risk of radicalisation or already radicalised. Causes and vulnerabilities need to be investigated.

Training is key

- Many participants reported that in training sessions there are often signs of unprofessional and intolerant behaviours or potential extremist attitudes. Concerns about racist, sexist, homophobic, anti-government opinions/expressions to explicit extremist viewpoints in support of violent extremist ideologies.
- **Training** is the place to hold discussions on the code of ethics, values and democracy.
- There was a good experience with dilemma training: a team has a group discussion together with their management to talk about their work dilemma's and how to deal with them. This will perform as an outlet for staff and if there are some issues, this can be signalled by peers and management in this way.
- Some suggested having training on the code of ethics.
- Small group trainings and systematic discussions on radicalisation should be considered as the preferred option.

Code of Ethics and high professional standards

All practitioners in police, prison and army swear an oath and adhere to some sort of Code of Ethics at the beginning of their career.

- There was a discussion on whether the Code needs to be renewed and signed again throughout steps in the career. In some countries, your potential promotion or transfer will always depend on the extent of adherence to the code.
- You either obey the high standards of the Code or not. It can and must be discussed in the training and in teams, to keep it alive and help staff internalise it.
- The code should be very pragmatic and concrete, for instance on what someone is allowed to say/express on social media or which institution/club/organisation to join.
- In most of the Codes of Ethics, there is strict neutrality and total absence of political choices or religious adherence. An officer cannot publish anti-government messages on social media platforms. It is normal that discussions inside the teams reflect discussions happening in broader societies. Such discussions could could be considered when designing trainings and updating the professional standards.

Leadership and Culture

In several parts of the discussion the participants asked attention for the important role of management, and their role in boosting a high standard and resilient culture, inspired by their leadership.

- There should be also mentioned the Strategy from the UK on the prevention of insider threats. It is the basis showing direction to the management and giving the priority for the preventive actions.
- Manifestations of inappropriate jokes and sending harmful memes. This is the grey zone that might look innocent but can have consequence. The grey zone and the unhealthy culture are not always opposed by leadership. There are two sides to this zone:
    - Dark grey zone: e.g. expressing extremism in WhatsApp but not taking violent actions
    - Light grey zone: e.g. xenophobic, homophobic, sexist and misogynist jokes and memes.
- One of the major risks is that organisations and their leaderships think they don't run the risk of an insider threat.

- There is the risk that management and the organisation in general turn a blind eye to signals or do not recognise it as a problem.
- Conditions under which staff work are challenging and they are often confronted with hostilities.
  - There is growing risk of feelings of xenophobia and clans in the organisation.
  - The experiences of participants show that leadership should be much closer to their first-line practitioners.

Recommendations

Based on the discussion, we can make a distinction between recommendations for staff and management and recommendations for training.

Recommendations for management and practitioners

- Look for unfamiliar behaviour, which can also be unprofessional behaviour.
- If management makes reporting a priority, then staff will feel the urgency to signal and share problematic/unfamiliar behaviour of peers. Such urgency should be shared by all stakeholders in the organisation.
- Do not think that initial vetting is enough, and do not assume that insider problems are not in your organisation. The training of new colleagues is an excellent opportunity to continue the vetting.
- Working in teams everyday makes that there is social control/cohesion among peers. Social control is useful to detect changes amongst one another.
- Have a holistic approach, for instance like the British programme CONTEST[1], covering all aspects starting with an emphasis on prevention by doing regular vetting and on-going discussions/trainings:
  - Start by improving the initial vetting procedure by examining the personal life circumstances your candidate lives in.
  - Create a culture of prevention with safe spaces to talk about one another's perceptions of different ideas and taboos. Organisations need to set standards/code of conduct for behaviour.
  - Dilemma discussions/training every few months with the group and team leader. Team leaders can observe how people think about things, to learn more about their peers. Management should also show vulnerability and discuss their own dilemmas.
    - Dilemma training is effective because it does not accuse anyone directly.
  - Build mentoring and coaching programmes for your staff. This helps to create a secure environment.

Figure 1 Pillars to create a resilient organisation[2]

[1] More on CONTEST, the UK anti-terror strategy can be found on https://www.gov.uk/government/publications/counter-terrorism-strategy-contest-2018
[2] Presentation of Dr. Marvin Gamisch, Polizeipräsidium Frankfurt am Main.

- Have trusted persons or safe spaces where you can discuss your own problems or concerns about a colleague.
- Small group training to raise awareness.
- There are four pillars or building blocks to build a PVE resilient organisation, as presented by the Frankfurt police department (see figure 1).
- There are job-related reasons that make police susceptible to radicalisation (see figure 2):

General risk factors	Specific background conditions
High emotional pressure for police officers working in hot spot areas/frustration in daily work	Lack of political education/lack of media literacy
Processes of group dynamics in hierachical organisations	Effects of social and political changes (rise of right-wing populism, increasing refugee movements)
Long-term negative expierence (police work is focused on negative aspects of society)	Private problems
Authoritarian law and order mentality	Ignorance of political offences

Figure 2 Reasons for Misconduct[3]

Recommendations for training

- Training prepares management to consider insider threats as a priority.
- Training should focus on the bigger picture and also include polarisation and societal tensions. These could be pre-conditions for radicalisation and extremism of staff.
- Training for the people who do the screening and recruitment on radicalisation.
- Train staff to see, understand and intervene.
- Training throughout the year: bottom-up training because input will come from the staff itself.

Relevant practice

In **Hessen, the Frankfurt/Main Police Department, initiated an extensive approach** in response to a couple of cases of right-wing extremist content in private chat groups of officers. It started with research to understand the mechanisms behind the unwanted behaviour followed up by three strands of activities.

1. Transparency Meetings (up to 200 participants), with a presentation of a political scientist about the media strategies of the New Right/Alt-Right and a presentation of memes/conversations with racist, antisemitic, etc. contents, that occurred within private chats of Hessian police officers. This was followed by Transparency Talks in which senior officers talk in small groups about the contents. A first meeting

[3] Presentation of Dr. Marvin Gamisch, Polizeipräsidium Frankfurt am Main.

was held in 2019 in the Frankfurt Main Police Department for senior officers as raw models. In 2021 it took place all over Hesse also for rank-and-file members, with the most meetings in Frankfurt.

2. A program of Training and Education on three topics:

   - Intercultural competencies (intercultural, Islam seminar, othering) and visits to different cultural groups and places
   - Political education: dealing with anti-democratic incidents in leading positions and visits to historical places.
   - Media Literacy: fake news and conspiracy stories in the news and preparing of guidelines for off-duty police officers on social media.

3. Social Responsibility

   - Engagement of a specialist for supervision as well as an organisational psychologist (psychological risk assessment)

Follow up

- The exact numbers and the degree of radicalised staff members is unknown. More reporting and research are needed about the scale and nature in the European States.
- Participants in the meeting talked about the army and former military officers involved in radicalisation. However, the outreach to participants connected to the Army was low. More overview is needed about radicalisation within the army and among veterans and former military officers. Additionally, a future small-scale meeting can further explore this topic.
- Participants suggested RAN Trainings about radicalisation and insider threat for police, prison and military in different European States.

Further reading

The Conclusions Paper of the RAN small-scale expert Radicalised police, military and prison staff (16 December 2020) presents the findings of the first and only RAN meeting on this specific topic.

The Combatting Terrorism Center at West Point (USA) published 'The Insider Threat: Far-Right Extremism in the German Military and Police', describing several cases. (June 2021)

The German magazine *Der Spiegel* published an investigative journalism piece titled 'The Dark Side of Power. Exploring Right-Wing Extremism in Germany's Police and Military' which gives detailed insights into cases of radicalisation in Germany's Police and Military. (2020)

On 5 February 2021, United States Secretary of Defense, Lloyd J. Austin III, announced a department-wide stand-down to address the problem of extremism in the ranks. The research brief Extremism In the Ranks and After, which explores data from the Profiles of Individual Radicalization in the United States (PIRUS) project, is intended to help in this effort by providing information on the military service backgrounds of individuals who committed extremist crimes in the U.S. from 1990 through the first eleven months of 2021.

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.