

05/08/2022

**CONCLUSION PAPER***RAN C&N: Digital Frontrunners in P/CVE**16-17 June 2022, Riga, Latvia*

# Digital frontrunners: Key challenges and recommendations for online P/CVE work

## Key outcomes

Working online has become increasingly important across almost all fields of work, especially since the outbreak of the COVID pandemic in 2020 when working from home became mandatory for many people. This is also true for work in preventing and countering of violent extremism (P/CVE), since radicalisation processes are increasingly taking place online. Types of P/CVE work that is being done online are, for example: early prevention, trend monitoring, individual interventions, and alternative or counter-messaging.

In the past year, multiple RAN Practitioners Working Groups have discussed online P/CVE work in their respective areas (e.g. RAN Local, RAN Families, Communities & Social Care, RAN Youth and Education, and RAN Rehabilitation). To converge the insights from those meetings and identify remaining challenges and the needs for practitioners in order to take the next step in their online work, the RAN Communications and Narratives (C&N) Working Group held a meeting on 'Digital Frontrunners in P/CVE' on 16 and 17 June 2022 in Riga, Latvia. The participants presented their own online P/CVE practice or project as a "digital frontrunner", and discussed in smaller groups what their current challenges, top tips and future needs are.

The key outcomes of the meeting are:

- There is a need to enhance collaboration and sustainable networking amongst online P/CVE workers, also foreseeing a possible role for the EU (platform, knowledge dissemination, funding, etc.).
- Important issues of privacy of P/CVE practitioners themselves as well as the target groups were raised.
- There is a need to better address mental health concerns of practitioners who are exposed to harmful content online on a day-to-day basis.
- Authorities and funders need to acknowledge the importance of online work P/CVE work and the practitioners doing this work, in order to pave the way for further development of online practices.
- The digital frontrunners are facing data access issues: on the one hand this is about dealing with information overload and information silos, and on the other hand barriers between practitioners and target groups (age/generational, technological) are making it difficult to keep up with trends and developments.

The remainder of this paper is structured slightly different than in other RAN Practitioners conclusion papers. The highlights and recommendations are combined. Each sub-heading consists of a major "need" in online P/CVE work that was identified by the participants. For each need, an explanation is given as to which challenges the need addresses, which top tips (or recommendations) already exist, and what ideas there are for the next steps in order to further address this need.

## Highlights and recommendations

When the group of digital frontrunners in P/CVE discussed the challenges they are facing, the image of a “jungle of challenges” arose — a jungle in which each practitioner is in a different place, with different challenges around them, but without contact between the practitioners. How is it possible to overcome this challenging situation? How can we gain a helicopter view? This paper attempts to provide a structured overview of different types of challenges, top tips for other practitioners to tackle (part of) these challenges, and the needs to address remaining challenges (i.e. to take the next steps forward in online P/CVE work).



### 1) The need for improved ways to keep track of online trends and recent research

One of the most important needs the digital frontrunners of online P/CVE work identified is the need for improved ways to keep track of online trends and to keep up to date with reports and research. Currently, keeping track of both online trends (what is happening online) and the cutting-edge research regarding relevant topics for online P/CVE work is difficult for practitioners. There are several challenges related to this:

- The most overarching challenge is the **lack of capacity**. Most of the challenges below are in one way or another related to a lack of capacity.
- **New platforms emerge constantly**, and the **relevant platforms change rapidly**. As a practitioner, it’s hard to keep track of which platforms are being used by different types of conspiracy thinkers, radicals and extremists.
- There are often **barriers between practitioners and their target group**, especially concerning young people. For example, age difference/a generational gap can make it difficult for practitioners to understand what concerns and worries young people. Moreover, the rapid development of technology is picked up by young people quicker than by practitioners.
- There are multiple challenges concerning **data and information**:
  - On the one hand, there is an **information overload**. The amount of data (i.e. social media posts on different platforms) is so vast that it’s impossible for practitioners to keep track of everything that is happening online.
  - On the other hand, there are **information silos**. Practitioners often work in their own area of expertise, focusing on only a small, specified portion of the available information online. This can lead to tunnel vision and missing out on potentially relevant information outside of the focus of a practitioner.
  - On top of this, there is often **limited access to data from platforms**. There are also discrepancies between platforms in terms of accessibility and availability of data, and the type of data that is provided. This makes it difficult for practitioners to process information from different platforms in a standardised way.
- A large part of what is happening online takes place **outside of regular office hours**. This makes it difficult for practitioners who have a day-time job but do online P/CVE work to keep up to date with what is happening online.
  - This can be applicable for several types of online P/CVE work. For example, Data collection in trend monitoring can be automated, but it often still requires manual assessment. People reaching out for counselling or to report hateful content might want to do this outside of office hours because that is when they are online themselves.
- There is a lot of relevant and recent research on the topics addressed by online P/CVE practitioners, but **there is no clear overview and a lack of access to this research**. This makes it difficult for practitioners to keep up to date on relevant research.

During the meeting, the participants identified one important top tip, or recommendation, to tackle some of the above challenges:

- **Cooperate**, not only with your direct colleagues but also with other organisations. Given the fact that there is a general lack of capacity, an information overload and organisations working in information silos, it is beneficial for all parties to share information regarding trend monitoring and relevant research between organisations and individual practitioners. **Do not reinvent the wheel** by doing the same work as a similar organisation and come to the same conclusions, but also **do not be afraid to cooperate and share information with each other**.

Moreover, several ideas to take the next steps in addressing this need were suggested by the participants:

- Regarding data access, it was suggested that **platforms** could provide **open APIs** (application programming interfaces) to researchers and practitioners so they can consistently access and use data from these platforms. Not only the big platforms but also fringe platforms need to think about how they can provide access to practitioners and researchers in order to prevent and counter radicalisation (within legal and ethical boundaries, of course).
- Also, **policy** and **funding** could play a role in overcoming these challenges, for instance by promoting collaboration and demanding data access.



## 2) The need to maximise opportunities for collaboration

The second major need identified is the need to maximise opportunities for collaboration and cooperation, both for practitioners and organisations doing online P/CVE work, on local, regional and (inter)national levels. There are several challenges that can be tackled by capitalising on opportunities for collaboration:

- As also explained in the previous section, the challenges relate to **monitoring trends and developments**, mainly concerning **lack of capacity**, **information overload** and **information silos**. By working together, you can divide certain tasks and increase overall capacity.
- **Time drain on bureaucracy and administration** takes away valuable hours that could be used to invest in cooperation and collaboration with partners. An example of this is the time spent on funding procedures. Moreover, funding procedures normally do not promote cooperation between different organisations (also see the next section on funding).

Several tips and recommendations were suggested by participants in order to address this need for more collaboration:

- **Identify the partners that can strengthen you and work across disciplines** (if not within your own organisation, then by collaborating with partners).
  - Also consider potential cooperation with **tech and social media companies**.
- **Use your network** and do not hesitate to reach out and ask for help.
- In *early prevention*, consider actions to **co-create** with your target audience (i.e. youths). Involve them in developing your online practice in order to reflect their needs (e.g. using their experience and preferences in social media use to create media literacy training) <sup>(1)</sup>.
- Do not be afraid to **share information** with partner organisations you cooperate or collaborate with (bearing in mind GDPR rules of course).
- Take the initiative to establish more **structural collaborations** and **sustainable networking** between your organisation and others.

<sup>(1)</sup> This is less relevant for countering violent extremism, that is, in a phase where individuals are already radicalised. It would not make sense to attempt co-creation then. Formers could be an alternative to involve.

In order to further address the need to maximise opportunities for collaboration, several ideas to take the next steps were brought in by the participants:

- Find ways to **safely share the information you collect** and analyse with your partners.
  - Consider making a **division of labour** with partners you collaborate with. If you provide them with pieces of information they are not gathering themselves and vice versa, you can strengthen each other.
- Related to challenges around funding (see the next section), a good way to start collaboration is to start **developing and proposing projects together with partner organisations**.



### 3) Need for more and improved funding

Getting the right funding was identified as a major need. There are several challenges related to funding that the participants experience, especially concerning the way funding is currently often organised:

- In general, it is difficult to receive funding for online P/CVE projects, so a general lack of funding is the main challenge.
- More specifically, participants identified the following problems with funding:
  - The **funding cycle** is often shorter than the desired project cycle or duration, making it difficult to completely execute a project or to have continuity.
  - Funders are often **geolocation-oriented**, meaning that they only fund projects that address a certain geographical area. The problem with this is that online P/CVE work is borderless and transnational, making it more difficult to justify to funders.
  - There is often a **mismatch between the funder's expectations and reality**, for example regarding measurable results. The results of online P/CVE work are especially difficult to measure. On the one hand, this has to do with the anonymity of the user, the difficulty to find out whether you are targeting the right people and the effect it is having on their behaviour. On the other hand, it is difficult to determine a causal relationship between the intervention and observed changes in online prevention, making it difficult to measure success or positive results.

Several tips or recommendations regarding funding are:

- Formulate and work with **achievable interim goals** that you can also communicate to the funder.
- Look for **funding from multiple sources** (not just one big funder) for your project, in order to ensure continuity despite the challenge of funding cycles.

Ideas for next steps in addressing the need for more and improved funding were primarily aimed at **opportunities for funders** to make changes in their funding processes to make it easier for practitioners to receive the type of funding they need. The recommendations for funders are:

- One of the ideas was "**funding without borders**", meaning to promote a new way of funding that looks beyond geolocation. This is especially relevant for online work since the online world does not abide to physical borders.
- Also, **multi-annual funding** aimed at (further) developing working methods and tools could help to ensure continuity of online P/CVE projects.
- Lastly, more **transparency** from the funders on the decision-making process, criteria of granting a fund, competing parties, etc. could benefit the work that is being done and stimulate knowledge exchange between the organisations that receive funding.



#### 4) More attention for privacy and mental health aspects for practitioners

A need that was broadly agreed upon amongst the participants is to give more attention to both privacy and mental health aspects of practitioners engaging in online P/CVE work. Practitioners face the following challenges regarding privacy and mental health:

- Practitioners engaging in online P/CVE work are being **exposed to hateful content** for a sustained period of time, straining their mental health.
- Currently, there is a **lack of psychological support** for practitioners doing online P/CVE work.
- Because of the above challenges, there is hesitation **to get started with online P/CVE work** amongst practitioners, while it is becoming more and more important to also be active online as a practitioner.
- In terms of **privacy for practitioners themselves**, the main challenge is how to ensure the safety and security of practitioners while maintaining effective online P/CVE work and being transparent about your line of work.
- Moreover, **privacy protection of the target group or clients** also poses challenges, mainly around access to data and transparency.

Top tips or recommendations identified during the meeting to address mental health and privacy are:

- **Create a safe space** for the team within your organisation. This is an important basis to bolster mental health and give practitioners the confidence to do their online work.
- Ensure **safety for practitioners during external (online) contacts**.
- Create a **mental health policy** for your employees. This could include limited hours of doing the actual online work and/or offering regular mental health support.

Ideas to take the next steps are:

- **Learn from adjacent fields**, especially regarding mental health concerns for practitioners. For example, learn from police inspectors who are detecting and screening for child pornography or speak to content moderators of tech companies about their working methods in this respect.
- With the team, create **guidelines and standards** for “online hygiene”, for example regarding the amount of time a practitioner spends online (being exposed to potentially hateful content).



#### 5) Need for professionalisation

Related to the need for more attention for privacy and mental health concerns amongst practitioners, the need for more overall professionalisation of organisations and practitioners doing online P/CVE work was also identified. This includes guidelines and procedures taking into account specific aspects of online P/CVE work. Several challenges are related to this:

- There is a **lack of recognition for the importance of online P/CVE work** on multiple levels, for example amongst other practitioners who are not engaging in online P/CVE work, funders and organisations and on the policy level.
- **Mental health and privacy concerns** are also challenges, as discussed in the previous section.

- **Keeping up with trends** is a major challenge, as discussed in the first section. Further professionalisation can help in creating more structure and capacity to do this.
- **Office working hours** don't align with what is happening online. Next steps are needed to have a more consistent coverage (like working in shifts/international collaboration working in different time zones, etc).
- Professionalisation can help take away the challenge of the hesitation **to engage in online P/CVE work**.

Top tips or recommendations for taking the next steps in professionalising online P/CVE work that were identified are:

- **Standardising training for online P/CVE practitioners** in the skills they need to do online P/CVE work can help in taking away the uncertainty regarding engaging in online P/CVE work. Concrete examples of what practitioners can be trained in are:
  - online/digital trends
  - media literacy
  - storytelling in online spaces
  - identifying your own biases
- Exchange of working processes, guidelines and procedures between online P/CVE practitioners and their organisations. Establish a **code of conduct** that applies to multiple organisations.
- Professionalisation needs the right combination of "wobble room" and structure. A code of conduct should provide structure, however it should not limit the **room for experimentation**.
- Another crucial part of professionalisation is doing proper **evaluation** and using this to further shape a **learning environment**.



## 6) Tips to get started with online P/CVE work

Next to the above five major needs that were identified during the meeting, there were also some general tips shared for every P/CVE practitioner to get started with online P/CVE work. These mainly concern challenges around finding the right message to share and how to reach and engage with your target audience. These general recommendations are:

- **Don't reinvent the wheel.** Learn from existing offline practices and translate them to online, learn from other existing online practices and learn from adjacent fields.
- The KISS principle – **keep it simple stupid**. Don't make it any more complicated than it needs to be.
- **Celebrate and embrace your failures** and learn from them. Do not be afraid to engage in online P/CVE work.
- **Combine online and offline in your practice.** For example, engage with your target group online initially, but invite them to an offline event or session at a later stage.
- **Know the language of your target group.** Use connecting but authentic language and behaviour, but also get to know the language your target group uses online and use this instead.
- In the case of *prevention* work: **co-create**. When developing your online practice, talk to your target group (e.g. youths) and involve them in order to reflect their needs.

- For *countering* work, it is more difficult to co-create with your target group, as it concerns individuals already radicalising or being part of an extremist organisation. One exception here is the possibility to include **formers** in co-creating intervention.

## Relevant practices

Two inspiring practices were presented digitally during the meeting:

**Debunkeu** (Lithuania): <https://www.debunkeu.org/>

Debunkeu is an independent technology think tank and non-governmental organisation that researches disinformation and runs educational media literacy campaigns. Debunkeu.org provides disinformation analyses in the Baltic countries, Georgia, Montenegro and Poland, as well as in the United States and North Macedonia together with their partners.

**Gaming with the police** (the Netherlands): [https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran/collection-inspiring-practices/ran-practices/gaming-police\\_en](https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran/collection-inspiring-practices/ran-practices/gaming-police_en)

Gaming with the police is a practice developed by the Dutch community police to keep in touch with youth who are active in the digital domain. By entering their “comfort zone” through gaming, police officers connect with the youth and earn their trust. This gives the police the ability (either in the group or in one-on-one interaction) to speak with the youth, help them with different problems they might experience, inform them and do a lot of preventive work. Engaging with youth through video games lowers the boundaries that youth feel regarding talking to the police and constitutes a unique means of trust building and new style “community policing”.

Moreover, all participants also presented their own project or practice in a 2-minute pitch-style carousel. These are:

- Sulis Insights: <https://www.sulisinsights.com/>
- Mediawijs: <https://www.mediawijs.be/nl>
- Local Police Rupel, <https://politiezonerupel.be/>
- Moonshot: <https://moonshotteam.com/>
- National Family Benefits Agency / Promeneurs du net: <https://www.promeneursdunet.fr/>
- OREAG: <https://www.oreag.org/>
- Youth Foundation Baden-Wurtttemberg: <https://www.jugendstiftung.de/die-stiftung/english/>
- BAG RelEx: <https://www.bag-relex.de/en/homepage/>
- Local Streetwork on/off: <https://www.localstreetwork-onoff.de/>
- Streetwork@online: <https://www.streetwork.online/>
- Legato: <https://legato-hamburg.de/>
- Socialife: <https://www.socialife.nl/>
- Textgain: <https://www.textgain.com/>
- True Friend: <https://true-friend.nl/>
- The Khalifa Ihler Institute: <https://www.khalifahihler.org/>
- One World Strong: <https://www.oneworldstrong.org/>

## Follow-up for RAN & recommendations for policymakers (EU and Member State levels)

---

During the meeting, several ideas and suggestions concerned a coordination on the EU and/or national level. As RAN Practitioners in its current form would not be able to provide for all of these ideas and needs, they might serve as inspiration for future EU development and/or the further development of RAN. The ideas and suggestions are:

1. Open up collaborations between organisations involved in online P/CVE.
2. Promote sustainable networking: facilitate connection between online P/CVE practitioners beyond current RAN Working Groups.
3. Create a platform for exchange / a safe space for online P/CVE practitioners.
4. Find different ways to share/disseminate cutting-edge information and knowledge on online trends and research findings.
5. Create a new RAN Working Group on (online) ethics and privacy within P/CVE.

Looking at some of the challenges mentioned during the meeting, especially those regarding privacy, another suggestion would be to look into **ethics and P/CVE** in a future RAN meeting. Some of the questions that could be addressed are:

- How is it possible to balance users' confidentiality and privacy with the need to safeguard the public? When is the infiltration of private groups justifiable? In which instances should information about the user be shared with public authorities?
- How can situations where the service provider's ethical principles clash with those of the project funder be handled?
- Should researchers and practitioners have a moral obligation to report extreme content found on social media platforms?

Next to these questions around ethics, and the need for mental health support that was expressed during this meeting, a future meeting could also address the topic of **legal advice and protection** for practitioners doing online work in the field of P/CVE.

## Further reading

---

- RAN Specialised Paper (March 2022): [Lessons Learned from Alternative Narrative Campaigns](#)
- RAN FC&S (March 2022): [Hybrid social work and digital awareness for family support](#)
- RAN Y&E (March 2022): [Integrating the online dimension into offline pedagogical practices](#)
- RAN Rehabilitation (February 2022): Exploring digital/hybrid exit and rehab work (paper to be published online).
- RAN Specialised Paper (February 2022): [Hybrid youth and social work](#)
- RAN LOCAL (May 2021): [An online P/CVE approach for local authorities: challenges, tips & tricks](#)
- RAN HEALTH (November 2020): [P/CVE and mental health support online](#)
- RAN C&N (November 2019): [Effective Narratives: Updating the GAMMMA+ model](#)
- RAN Webinar on [Evaluations of strategy and interventions on local level for local coordinators](#)
- RAN Small-scale meeting (March 2021): [Effective and Realistic Quality Management and Evaluation of P/CVE](#)