Radicalisation Awareness Network
RAN Practitioners

Veb-stranica: ec.europa.eu/ran

twitter | facebook | linkedin | youtube

CONCLUSION PAPER
RAN LOCAL
16-17 June 2022, Barcelona, Spain

How to deal with the local impact of online (extremist) activities

Short summary

The digital ecosystem is becoming both ever more complex and therefore equally important for practitioners to understand. It is one within which vulnerable audiences spend time, socialise and consume information, within which terrorists and extremists radicalise and recruit, and within which practitioners must do their work.

As concluded in previous RAN (LOCAL) events, online prevention and countering of violent extremism (P/CVE) work should not be considered an 'extra' to the offline work. One should not only look at either online or offline interventions but also how they interact and how online activities influence the local context – be it at schools, within communities, at demonstrations, etc. In theory, the development of online activities offers great possibilities and opportunities, including for educational and prevention work. But in practice, not all professionals feel at ease with the online environment, and the transition from offline to online requires special attention and effort. It should therefore be an integral part that is embedded through a holistic approach in local P/CVE work. However, being able to intervene online and to deal with the 'offline' consequences of online activities through a holistic approach is highly challenging for local coordinators and practitioners. On 16 and 17 June 2022, local P/CVE coordinators came together with other practitioners and representatives from NGOs to discuss two sets of challenges that local coordinators indicated to be struggling with. For both sets, participants shared with each other what they are facing on the local level, why this is challenging to them and how they (try to) deal with these challenges.

Some recommendations that participants proposed to deal with the identified challenges:

- Do not fear General Data Protection Regulation (GDPR) regulations – find a way of working with them, rather than against them.
- Review and update the local multi-agency structure's partners and agreements previously made to include the digital ecosystem – e.g. make new agreements about sharing information from online sources.
- Invest and professionalise in including the digital ecosystem within practitioners' knowledge and skill sets.
- Digital resilience and media literacy (including knowledge of algorithms and filter bubbles) should continue to be taught not only to children but to anyone navigating online.

Context of the discussion

With new digital technologies and platforms being introduced and adopted at a high pace, people – both young and old(er) – are spending more time online than ever before. Technologies like virtual reality and AI reinforce the melting together of online and offline worlds, of placing them on a continuum rather than seeing them as two separate worlds. The COVID-19 pandemic has accelerated this digital transformation, as well as the challenges this brings. Vulnerable audiences are spending more time on news sites, social media channels, video gaming platforms and chat rooms. They are thus more easily targeted by terrorists, extremists and other malicious actors who proliferate large amounts of disinformation, fake news, conspiracy narratives, extremist propaganda, hate speech and much more. The digital ecosystem is becoming both ever more complex and therefore equally important for practitioners to understand. It is one within which vulnerable audiences spend time, socialise and consume information, within which terrorists and extremists radicalise and recruit, and within which practitioners must do their work.

The need for online interventions by practitioners has been addressed in previous RAN (LOCAL) events. As concluded in the RAN paper 'An online P/CVE approach for local authorities: challenges, tips & tricks', online P/CVE work should not be considered 'extra' to the offline work. One should not only look at either online or offline interventions but also how they interact and how online activities influence the local context – be it at schools, within communities, at demonstrations, etc. It should therefore be an integral part that is embedded through a holistic approach in local P/CVE work.

However, being able to intervene online and to deal with the 'offline' consequences of online activities through a holistic approach is highly challenging for local coordinators and practitioners. This meeting focused on two sets of challenges that local coordinators indicated to be struggling with. For both sets, participants shared with each other what they are facing on the local level, why this is challenging to them and how they (try to) deal with these challenges.

Legal aspects, localisation, monitoring and information sharing

- Construct a clear overview of how extremist content and activities travel online and the implications of this on a local level. In many countries, the **mandate for monitoring online content lies with the police**. Subsequently, partners in a multi-agency setting therefore depend on resources, willingness and possibilities from the police to share information.

- In the same context, many participants indicated that an inadequate or **unclear legal basis for sharing information** derived from online sources undermines their effort to conduct online P/CVE work. For some, the lack of a clear legal structure means that information from online sources or activities cannot be incorporated in multi-agency prevention work. Many also indicated to be operating in a **grey area** between, for example, safeguarding freedom of speech and preventing hate speech, which seems to be a particularly fine line in an online context.

- At the other end of this spectrum, local coordinators struggle with a strict interpretation of existing regulations, like the GDPR. Out of **fear of breaching the GDPR**, multi-agency partners are reluctant to share any personal information at all. Some practitioners are additionally reluctant in sharing concerns with police, as they fear that an investigation in online behaviour ends up in a police file and leads to **stigmatisation**.

- Fake news, conspiracy narratives, extremist propaganda and hate speech could be posted from anywhere, even though they can target or have effect in a local community. Local coordinators indicated that this makes it difficult to go after the perpetrators and to establish who is responsible for doing so when they are outside of the local jurisdiction.

One of the examples mentioned that explains how information sharing in the absence of a clear legal structure presents an obstacle for P/CVE coordinators and practitioners:

An NGO or P/CVE practitioners have some concerns about potential suspects who have done nothing illegal, but they had, for example, some connections with people who travelled to Syria to join ISIS and now they are active on social media platforms. The P/CVE practitioners have no legal basis to monitor the internet activities of these suspects, so they have no idea in which online groups these suspects are or which websites they regularly visit. Therefore, they reach out to the local police who have authorisation for monitoring. They express their concerns and ask for more information to see whether they should intervene or not. However, the police, whether due to the investigation confidentiality restrictions or GDPR regulations, are not always willing or able to share information with other partners, which leaves the practitioners in the dark regarding the internet use of the people concerned. They miss a puzzle piece of information from a person's life and behaviour.

Knowledge, skills and interventions from and by first-line practitioners

- The main challenge regarding these aspects lies in local P/CVE coordinators' and first-line practitioners' **skills and knowledge of social media usage** and in **being able to identify content referring to extremist ideology**. This requires being able to navigate different social media platforms as well as knowledge of symbols and language used within different extremist ideologies on these platforms. With an average of 7.4 different social platforms that a person uses where they spend nearly 2.5 hours per day ([1]), it is a lot to keep track of.

- The lack of knowledge and skills is not only limited to interventions or detection skills. Practitioners also face the difficulty of having access to the **right technology and expertise** to develop and launch suitable interventions, awareness-raising programmes or alternative narrative campaigns online.

- Practitioners struggle to **keep track of online developments**. This is not only because of technology and platforms that develop at a high pace, but also because extremists are embracing new strategies swiftly to stay undetected or to stay just within the margins of the law.

- When first-line practitioners spot signals of extremist content, they don't always know what **course of action** this requires. Should they report it, to whom, should they engage with the person posting, or would that only feed the algorithm? Are they allowed to interact from their personal profile or should they have a professional profile?

- Another aspect of this challenge is **identifying the target group when intervening online**. It is incredibly difficult for practitioners to identify the most radical elements within a group from other members who are still willing to engage in substantial debate and participate in a face-to-face intervention. Transforming online communication with vulnerable individuals into a face-to-face setting requires special skills and tools to create a trustful relationship with the target audience to subsequently challenge their ideas and views.

One of the examples mentioned regarding the challenge of lacking skills and knowledge:

How can local P/CVE coordinators support first-line practitioners in professionalising in the online ecosystem in a sustainable and structural manner? Especially when working on prevention and strengthening resilience, a local coordinator indicated to be struggling with the balance between training, funding, education and prevention in the broad sense. Ideally, they wish their entire population to be digitally resilient, but resources are always limited. Especially with the amount of content being published, there is no capacity to monitor

([1]) Statistics derived from: https://datareportal.com/social-media-users

everything, so the work of prevention becomes even more important. Still the question remains which professionals in particular need training, how this can be done, where should they look (which groups are most at risk?), when should they intervene themselves, and what should be the balance between online and offline?

Recommendations

It was agreed upon that **local P/CVE coordinators play a pivotal role** in detecting and monitoring online activities and making the transition to reaching out to individuals at the local level. They are the ones who can connect information from different stakeholders involved and subsequently decide who or what is the best way to reach an individual of concern, as they know the local field. Regarding the two sets of challenges discussed at the meeting, some recommendations for local P/CVE specifically, as well other partners in a local multi-agency structure, were formulated.

Legal aspects, localisation, monitoring and information sharing

- **Do not fear the GDPR.** Find a way of working with it, rather than against it. For early, primary prevention, the GDPR shouldn't be an obstacle. As **primary prevention** doesn't focus on individuals, so no personal information has to be shared. When it comes to **secondary or tertiary prevention**, rules can be established and agreements signed on how and when personal information is collected and shared within a multi-agency framework. To protect people's privacy, concerns can be shared anonymously. Another option sometimes lies in practitioners reaching out offline and not registering personal data of the people they talk with.

- To include the online dimension as an integral part of P/CVE work, it is worth **reviewing your local P/CVE action plan and multi-agency cooperation structure**. Do your earlier defined (sub)goals still apply, or do they require adjustment to include an online setting? How about the definitions used? Do you still have the right partners included to prevent and counter violent extremism? What are everyone's roles and responsibilities in the multi-agency structure, both online and offline? Is there a difference in the sharing of information retrieved from online sources compared to offline sources, and, if so, how can it be shared? Where needed, discuss, **review and update the agreements** previously established with the different partners involved in the multi-agency structure ([2]). Practitioners' organisations can do the same by establishing rules on who can intervene online and how ([3]).

- **Be clear and communicate** to all actors involved in the multi-agency structure how and for how long (personal) information is saved. **Transparency and trust** remain key factors in building and retaining effective collaborations.

- Reviewing the roles and responsibilities of the partners involved in multi-agency cooperation should also include considering the **localisation of online perpetrators** and who is responsible within which jurisdiction. As online content is not limited to borders, especially not the local level, it will be helpful to know who to contact when follow-up is required beyond the local level.

- The **local P/CVE coordinator** can be the person to bring different partners together and who can inform all relevant partners of who or where to reach out to with questions. The idea of establishing an **'info hub'** was given, a (digital) place to consult where good online resources can be found that practitioners can consult when they miss certain knowledge, skills or expertise.

([2]) For information on setting up multi-agency structures and agreements, see, for example, the ex post paper RAN LOCAL (2018) 'Tabletop exercises: Practicing multi-agency cooperation' and ex post paper RAN LOCAL (2017) 'Local Action Plan Academy'.
([3]) See, for example, this paper on How to do digital youth work in a P/CVE context (RAN, 2020).

Knowledge, skills and interventions from and by first-line practitioners

- **Invest and professionalise in including the digital ecosystem within practitioners' knowledge and skill sets.** Besides training, this could be done by filling current knowledge or expertise gaps within a team through hiring either external expertise or reinforcing the team with an 'online talent'. Although digital expertise is not solely found within the younger generation, who have grown up with social media, they can provide valuable expertise and might be closer to the target audience. Reinforcing digital skills can help, for example, social or youth workers to gain autonomy in navigating the online world and to feel more secure in doing so, rather than being dependent on young(er) people telling or helping them to find out what's happening online.

- **Digital resilience and media literacy** should continue to be taught not only to children but to anyone navigating online. It is important for people to be aware of how the digital ecosystem works, what the effects of **algorithms** and **filter bubbles** are, and how extremists try to influence these. This could be a combined effort of awareness-raising campaigns (by NGOs), training and education by practitioners, as well as public–private partnerships between governments and social media companies to limit extremist influences online.

- As independent actors, **NGOs can be of crucial importance and added value** in raising public awareness through (alternative narrative) campaigns and specific training or education on topics like media literacy, digital resilience or even democratic values as they might be more credible to the target audience.

- Local and national governments can support NGOs and practitioners through the **funding** of different campaigns and interventions. In preventing violent extremism, it is important to try and establish not only what works in which context but also to establish long-term effects and funding. This requires careful consideration of which interventions and partners to fund, and to monitor and evaluate if the available funds are well spent.

- What happens online often has an offline outlet too, and vice versa. P/CVE practitioners should try to **balance this two-way stream** of online/offline action and reaction. This goes for interventions as well as **linguistics**; be aware that terms used online are not always the same as offline, even though people talk about the same subject. In terms of linguistics, **artificial intelligence** (AI) can assist in detecting extremist content and how it evolves to stay within the margins of the law and within the user regulations of the social media platforms. However, the amount of content disseminated and spread online is so big that even with the help of AI we cannot detect all malicious content. Prevention of a breeding ground for radicalisation leading to violent extremism therefore remains of utmost importance.

- Invest in the creation of **digital safe spaces**, such as digital democracy houses. These provide an online fictional world for people who have something in common, like a sport or a hobby. They meet online and subsequently can come together in a place in their city and learn to establish understanding and recognition for each other's perspectives and have discussions in a respectful manner.

Relevant practices

Safe Digital City – pilot project from Nordic Safe Cities

To help local P/CVE coordinators understand the specific landscape and patterns of how hatred, extremism and racism travel online in a geographical area like a city, Nordic Safe Cities has started a pilot project. Based on an algorithm that analyses open and public content on several platforms within the local digital landscape, local coordinators get a better grasp on who the hatred targets, what themes are polarising the debate and what triggers the hate. Not only does this help them understand what is happening, it also provides them with the tools to come up with specific interventions and to strengthen the local digital prevention of extremism. Examples of such areas of interventions under development could be: creating a digital team in the municipality that is responsible for analysing online hate and training prevention workers to work online, helping civil society organisations in working with an online moderate voice to counter online hate speech, or even ensuring safe local politics and a non-polarising and inclusive debate climate.

Follow-up

- For local coordinators, it would be useful to have a specific meeting or workshop during which each participant is asked to make a concept of how their local multi-agency structure can be adapted to include the online ecosystem as an integral part of P/CVE work, including ways of information sharing and roles and responsibilities of the partners involved.

- A webinar for local P/CVE coordinators on the latest online trends and developments in Europe and what this implies for local P/CVE action plans and interventions.

Further reading

RAN Local authorities Working Group (RAN LOCAL), 2021: An online P/CVE approach for local authorities: challenges, tips & tricks

RAN Local authorities Working Group (RAN LOCAL), 2017: Ex post paper Local Action Plan Academy

RAN Local authorities Working Group (RAN LOCAL), 2018: Ex post paper Tabletop exercises: Practicing multi-agency cooperation

RAN Youth, Families & Communities and RAN Communications & Narratives Working Groups (RAN YF&C and RAN C&N), 2020: How to do digital youth work in a P/CVE context: Revising the current elements

Strong Cities Network (2022): Together for Safety 2022 Online Talks | Key Findings