05/08/2021

CONCLUSIONS PAPER

RAN POL working group meeting – Community police and the online dimension
5 July 2021 09.30 – 13.00 CET and 6 July 2021 09:30 – 13.00 CET, online

Community police and the online dimension

Key outcomes

Community police officers are a highly effective asset in preventing and countering radicalisation leading to violent extremism and terrorism (P/CVE) at local level. Since extremist discourses are increasing online, community police officers must also focus on this digital space. Digital community policing (DCP) means curating an online presence and ensuring police are visible and approachable to their communities: following and engaging with these communities helps police remain informed and aware of prevalent problems.

In an online meeting on 5 and 6 July 2021, police officers and experts discussed what community policing looks like today, the response to the online dimension in police work, the various experiences of DCP, what competences and tools are required, and what training is needed.

The key outcomes are as follows.

- It is promising to see an investment across Europe in **innovation in community policing**, as this is crucial to keeping police involvement in P/CVE up to date.
- Following the shift online of the general public and subcommunities is essential for community police officers, but it also presents opportunities: **going online will keep officers engaged** and abreast of developments in their area and their communities.
- There are promising examples of DCP. For community police officers to be effective online, police need to invest in **training and tools**; they can gain from cooperation with academia, the private sector and NGOs.

This paper summarises the discussion at the online RAN POL meeting held on 5 and 6 July. It starts by presenting the highlights of community or proximity policing in P/CVE, with examples of how police in Europe are incorporating the digital domain into their work. After considering what DCP could look like, the paper reviews the required competences and training. The paper concludes by describing practices of interest, and also makes recommendations and provides suggestions for follow-up and further reading.

Discussion highlights

- Staying abreast of developments, knowing the subcommunities, building a network and being accessible are key elements of community policing. As most communities and subcommunities now meet and communicate online, community police should follow this trend.

- DCP is still relatively new: police officers need to explore what DCP could look like and can learn from the experiences of others.

- In the Netherlands, there are around 50 community police officers, 50 % of whom are digital community police officers. There is a national network as well as centralised training programmes for different dimensions like online investigation, the Dark Web and staying safe. DCP is distinct from the cybercrime units. The community police officers, who work for 50% digital and 50% on the streets, are not restricted to examining crimes, but have a broader overview, which is helpful in understanding current events and trends in communities and relates more to P/CVE. (For more information, see the section on inspiring practices.)

- Digital police officers gather information, enter it into the police records system and forward it to the appropriate colleagues (for instance, cybercrime units). Digital community police officers function like spiders in a web: they do not undertake a complete investigation but rather act to signal and refer signals on. They are authorised to view open profiles, and may make a special request to view closed profiles.

- DCP focuses on connecting the world, the web and the neighbourhood. Signals online are reflected in the streets and vice versa.

- Open-source intelligence is more in line with generic, preventive police work.

- The Norwegian police upscaled a pilot of an Internet Patrol Unit (featured in a 2018 RAN POL meeting) to an approach where all 12 regional units now have such an Internet Patrol Unit. Three-person patrols are active on different platforms and channels. (For more information, see the section on inspiring practices.)

- DCP development is an ongoing evolving process taking place in a national context, in line with the character of a given police force and consistent with societal developments.

    - To date, some Member States have not (yet?) implemented DCP or even community policing without the digital component; others have experimented considerably and have programmes and protocols in place. Spain and Portugal have promising new community policing projects: in Lisbon (PT), the community partners approach is being redesigned to include decision-making initiatives with stakeholders from the community; in Xabia (ES), under proximity policing, significant effort is being invested in training, including training on extremism.

- DCP is about:
    - being seen;
    - being approachable;
    - anticipating and reacting to threats that are typical or that are transferred to an online environment;
    - adopting a preventive perspective, as compared to the role of crime investigator;
    - being an indispensable element of information-based, area-focused policing.
- The Belgian Community Policing and the Prevention of Radicalisation (CoPPRa) project provides three-day-training sessions on community policing and information sharing, including extremist ideologies, organisations, radicalisation processes and indicators. CoPPRa has been implemented in other Member States, sometimes in an altered form.
    - The CoPPRa training programme integrates new phenomena and current/actual (geopolitical) events.
    - It touches on different social media platforms and propaganda from various groups, and on the effect of the Covid-19 pandemic discourses online.
- The European Union Agency for Law Enforcement Training (CEPOL) offers a wide range of training programmes of interest for police forces investing in digital competences for P/CVE.
    - The EU Strategic Training Needs Assessment (EU-STNA) was commissioned by CEPOL to identify gaps in knowledge, skills and competences, and training needs. Its main goal is to support, develop, implement and coordinate training for law enforcement officials.
    - The online CoPPRa module illustrates how police can build relationships with the community through interaction with local agencies and members of the public, enhances the capacity of police officers to identify risk factors and indicators that can lead to radicalisation as well as pre-incident indicators, and highlights EU and other international initiatives and networks in this field.
- The Belgian national Internet Referral Unit (IRU) carries out internet searches and investigations. The IRU works alongside local and federal police, and Europol.
    - The Belgian IRU also removes harmful content from the internet. Working with Facebook, for example, is important for achieving this.
    - Internet investigation in Belgium often starts with (national?) IRU identification and case analysis, and then moves to the investigators and/or community officers.
    - The Belgian IRU investigates open sources with fake profiles. Interaction is not permitted, whereas digital community officers from other countries and the Norwegian Internet Patrol do engage online with individuals and communities.
- The role of the digital community officer within the community entails web care (accessibility), investing in contact with the target audience, education (prevention), and proactive open-source intelligence (OSINT), signalling and investigating.

- The role of the digital community officer in the police entails information-sharing (information about crime) and providing the digital sources of information (online trends, social media platform usage, cybersecurity).

- Key training points for digital community officers: communication with communities as well as colleagues from other units (online language): using social media (popular platforms) and other tools, recognising neighbourhood online networks: monitoring OSINT basics (gathering information online safely): cyber awareness and cybercrime basics; developing and improving digital competencies.

Recommendations

- To stay abreast with developments in their communities, digital community police officers need to:

  1. know their communities, and be aware of their online practices and what (street) language they use online;
  2. team up with local partners who are familiar with these communities;
  3. know what kind of platforms they use;
  4. keep their profile safe;
  5. build networks of trust, strive to be approachable to communities, and communicate on a normal tone online and offline with youngsters and subcommunities to build trust.
- Police need to invest time and resources in developing, testing and evaluating DCP.

- Community policing units need officers with competencies, tools, time and training if they are to remain up to date.

- When selecting digital community police officers and the determining the selection procedures, take into account competencies and the motivation to work online.

- Cooperation with NGOs and young people is needed to remain abreast of new digital trends and communications. Invite and incorporate private companies, NGOs and young people to digital community police training sessions.

- Before working online, community police officers should know how to protect themselves online and how to protect their profiles. Training in cybersecurity is important.

Relevant practices

The relevant practices from the meeting are outlined below. The concept of DCP varies across countries.

1. **Dutch Community Police Officers ([1]), the Netherlands**
   Each regional unit has the option to appoint one of its regular community police officers to become a digital community police officer (50 %). At the moment, there around 50 digital police officers, and they have formed a network. The Dutch police tendered a nation-wide training programme for digital police officers.

2. **Internet Patrol Unit, Norway**
   All 12 regional units in Norway have an Internet Patrol Unit. In this three-person unit, Operator One engages with individuals and groups in spaces like Discord and Minecraft, through a 'blue police profile' rather than as an identifiable individual officer with a face and name. Operator One is supported by Operator Two, who carries out the relevant open-source intelligence. The third member of the patrol unit is the team leader who oversees the operation.

3. **Web Constables, Estonia**
   In Estonia, web constables are police officers operating actively on Facebook with 'personal' police profiles. With their names and profile pictures visible, these officers are welcoming, approachable and easy to contact for citizens, especially minorities. Thanks to their Facebook profiles, the web constables are not perceived in the same way as the more 'daunting' police patrolling the streets. Both male and female citizens find it easier to contact the web constables. The Facebook police patrol online, seeking harmful content and interacting with citizens to remove it.

4. **Xabia Proximity Police, Spain**
   The proximity police are an integral part of the local or municipal police: they bring police closer to the different communities and neighbourhoods that increasingly require assistance and services. The online dimension enables the assessment and quantitative and qualitative improvement of the proximity police. The proximity police officers follow a three-step guideline: Step 1 entails developing community police skills through training, Step 2 entails achieving community integration by engaging with local communities, and Step 3 entails addressing needs and problems through constant evaluation.

5. **The Lisbon Community Police Model, Portugal**
   The Lisbon community police (CP) model is a community-based participatory planning approach for building safer neighbourhoods, partly through online work. The model is preventive, proactive and participative. It is run through joint planning and operation thanks to a local partnership between local police and communities, in a four-step process. In Step 1, a local partnership is established and named as the security group. In Step 2, the partnership undertakes a local security needs assessment in the community. In Step 3, the partnership designs the CP team's ideal profile for the given neighbourhood. Step 4 entails the recruitment & training of the CP team.

([1]) For more information on Dutch digital community police officers from the national police website, see https://www.politie.nl/informatie/de-digitaal-wijkagent.html

Follow-up

- One of the needs in DCP is more in-depth and extensive training for digital police officers. What should the training include and who should provide the training? Who are the officers the trainers are reaching?
- DCP could benefit from cooperation and collaboration with bodies outside the police field: how could private companies and academics become involved in DCP?

Further reading

The following texts offer further reading on the implementation of DCP in a P/CVE strategy.

The Internet Patrol Units in Norway focus on the police presence on the internet and social media, with additional information on cybercrime.

The role of police online in PVE and CVE is a 2018 RAN POL ex post paper describing the first RAN POL meeting on combining offline and online police work.

The RAN *Spotlight* magazine has dedicated its April 2021 issue to Digital Challenges for practitioners, discussing aspects such as digital transformation and online gaming.

R. Pelzer's article, 'Policing of Terrorism Using Data from Social Media', was published in 2018 in the *European Journal for Security Research*.

One-to-one digital interventions is a 2016 RAN C&N ex post paper considering how practitioners can directly reach young people expressing interest in extremist content online. The paper discusses the challenges, tips and ideas on online narratives and working.

How can online communications can drive offline interventions? is a 2018 RAN C&N ex post paper providing practitioners with tips and tricks on how to work online as a complementary practice to offline work. This is also the case for digital community police officers, who should be working 50 % online and 50 % offline.