RAN POL

EX-POST PAPER

The role of police online in PVE and CVE

It takes a network to defeat an extremist network

We cannot leave the online world to extremist networks. The police – already very active in dealing with extremism offline – need to extend their activities to the online world. Internet Referral Units, the Norwegian Online Patrolling Unit and Facebook police officers are showing the way in terms of combining online and offline work.

It is a game of 'notice and take action', wherein the action is not merely taking down. It also encompasses strategic analysis, communication and prevention, including anti-hate campaigns.

We need to counter, disturb and remove messages that push people in the wrong direction. And at the same time, we need alternative and other, positive messages.

Police will benefit strongly from investing in networks involving NGOs and the internet industry.

This paper was written by **Steven Lenos and Lieke Wouterse**, RAN Centre of Excellence.

Introduction

Social media are a major asset for extremists. Police attempting to prevent and counter extremism cannot leave the online dimension untouched. But what are their options? In this paper, we introduce some approaches that police could use as part of their online contribution to preventing and countering violent extremism online.

This paper is written for police wanting an overview of their online PCVE options, and is based on the RAN POL meeting on 'The role of police online' that took place on 1-2 March in Oslo.

After a scene-setter that stresses the need to counter extremists online, we discuss the different dimensions of noticing and taking action, as well as understanding and prevention. Since police cannot do this alone, we also discuss cooperation with NGOs and the internet industry.

Online matters

There are several reasons why police presence online matters. Even though the so-called Caliphate may have lost its territory, extremist jihadist ideas have been let loose and are being kept alive in the cyber-Caliphate. For Daesh, online jihadism is as important as the battlefield. Online jihadism supports physical jihadism. Daesh – and Al-Qaida – use the internet to propagate their ideology and spread a message of terror in order to polarise communities and mobilise, recruit and radicalise supporters.

It is not only global jihadist networks that have shown that they know how to use social media to their advantage. Right-wing extremists do too. For decades now, Stormfront, Daily Stormer and other platforms have been the digital clubhouses and echo chambers of right wing extremist ideologues and angry and vulnerable individuals. The alt-right infosphere is effective in spinning and framing information, and creating information bubbles to disseminate fake news and other propaganda.

The internet allows groups and individuals to establish networks of like-minded people, that can inspire and educate each other.

The Institute for Strategic Dialogue (ISD) recently published the research paper '*The fringe insurgency*'[1] that reports on international extreme right networks: *"Extreme right networks use military and intelligence resources such as leaked strategic communication documents from the GCHQ and NATO to run campaigns against their own governments. By staging sophisticated operations in the style of military psychological operations (or 'psy-ops'), they seek to disrupt democratic processes in Europe (…)."*

Terrorist attacks are also committed by lone actors. But these individuals are actually embedded in an infosphere and network of extremism. The internet plays an important role in radicalisation and self-radicalisation. Some lone actors execute their atrocities on instruction, but others have simply been inspired and act more or less on their own. This leaderless resistance is driven from within the online sphere, alongside calls to action for lone wolves. Individuals can find suggestions for targets as well as advice on how to execute attacks.

[1] The fringe insurgency. Connectivity, Convergence and Mainstreaming of the Extreme Right (2018) to be found on https://www.isdglobal.org/wp-content/uploads/2017/10/The-Fringe-Insurgency-221017.pdf

In place: internet monitoring

Internet Referral Units (IRU) are central to the police's online approach to monitoring. The IRUs focus on two important aspects of online propaganda: delivery and messages. It is important to monitor, understand and take action. Monitoring is essential in knowing what terrorists are doing online, it helps police understand what is happening on the Internet and what might happen in the real world sometime soon.

Europol's IRU is a major contributor to the EU Internet Forum's 'Database of Hashes', together with the internet industry.

To understand and refer online extremist or terrorist content, IRUs use semi-automated systems combined with human assessment. There is a constant investment in technological development. The 'buttonology' – tools like programmes to scrape, scan and assess networks, users and content – that is necessary to prevent and counter violent extremism (PCVE) online, needs to keep up with the evolving complexity of the internet and the platforms and technologies used. But the technology cannot do this alone, we need the human intelligence and assessment too, both in the development of the tools as in the assessment of online material.

When IRUs detect messages or persons of interest online, they can start a judicial investigation or make a referral to Internet Service Providers, asking them to remove certain content or close an account. Public-private partnerships and cooperating with the industry or other organisations is therefore crucial for online PCVE.

Access to EUROPOL's expertise is possible through the restricted online environment 'Check the Web'.

Bridging the online-offline gap

There is continuous interaction between online and offline. This is reflected in the Europol IRU's two workstreams, as well as in those of national IRUs. One workstream focuses on monitoring and searching the net, and making sure action is taken when something is found. Action can be an urgent response if a threat is imminent, removal of content, or investigation and prosecution. The work of Europol is done in such a way that it can be used for prosecution in court.

The other workstream involves responding to calls for support from police who need expertise, information or other assistance in relation to a suspect's digital activities to better understand both delivery and messages.

Norway has an interesting approach to bridging the gap between online and offline policing. The National Criminal Investigation Service (NCIS) has established an online presence on several platforms, and has a Cyber Patrol on Facebook. The Cyber Patrol has both a Facebook-police-page and a Facebook-police-profile. The police page is live on Facebook, while the profile is still in testing.

The Facebook page is a uniformed Police presence that engages the public in different ways. The police is presented in an open, uniformed, preventive manor. It can be compared to a physical police station, where people can contact the police. The page has two main functions:

1) to answer questions and assess tip-offs sent from the public through personal messages.
2) to publish posts with content on various topics, such as PVE and guidelines for young people, parents and adults.

The content reaches thousands of people. The overall objective of the project is to create a method and guidelines for online preventive policing in Norway. Based on experiences gathered so far, all 12 police districts in Norway

will implement an online preventive police presence in 2018.

The Facebook profile will be an operational online police patrol. The objective is to have an open, uniformed and preventive presence online. One of the focus areas will be fighting radicalisation and violent extremism. The intention is to raise awareness of criminal and/or worrisome behaviour in closed groups and encourage admins and/or platform owners (in this case Facebook) to remove illegal material. The police-profile is currently undergoing testing.

The need for understanding: strategic analysis and strategic communications

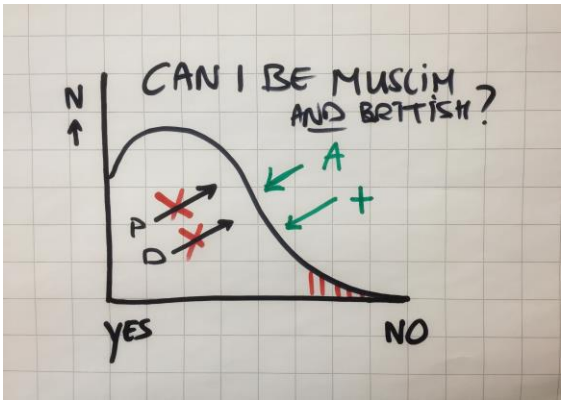
For Europol and police, the ambition is to bridge the gap between prevention and investigation. How can the two tasks support one another? Noticing and taking action are at the core of police internet activity. But just as important is the effort to analyse and understand online developments. There has been an evolution in the way extremists use messages – and in the technology used to disseminate them. Police need to be aware of these changes and at least try to keep up to date, or even be one step ahead of the extremists.

Understanding developments online is about understanding the changes in messages and delivery. Europol uses different technical assessment tools to monitor the online world. These are built with human intelligence and in cooperation with industry, local referral units and academia.

"The radicalisation problem is a communication problem. It is all about perceptions, and shifting them to realilty through communication."
(Hugo McPherson, ESCN)

Analysis of confiscated mobile phones and laptops belonging to radicalised individuals found mainly non-violent content, including Daesh propaganda on the brotherhood, belonging, and the opportunities in the Caliphate. This suggests that the belonging and not the beheading is appealing for, which shines a light on the type of content that contributes to radicalisation. This knowledge is important in preventive efforts, such as designing alternative and counter messages.

As suggested by the ESCN at the Oslo meeting, radicalisation can be seen as a communications problem. People buy into jihadi or other propaganda because of their perception of the world and their role within it. Through communication, we should, in response, be able to shift that perception to reality. An example.



The figure above shows how an imaginary population might have a range of views. On the left are people who fully agree with the notion that someone can be British and Muslim at the same time [2]. Then there is a portion that might

[2] This image could also been read as can someone (my neighbour) be British and Muslim at the same time.

wrestle sometimes with combining the two identities. And on the right are the people who strongly believe the Daesh propaganda that one has to choose: you cannot combine these two identities and you are either with Daesh or against Daesh, you are either a true Muslim or not. On this side of the spectrum are people who are vulnerable to radicalisation or recruitment. The problem with propaganda, but also hate speech and other negative and dividing messages, is that they push parts of the target audience to the right of the graph. So we need to counter, disturb and remove messages that push people in the wrong direction. At the same time, we need alternative and other positive messages that contribute to a shift to the left of the graph.

Investing in online resilience = crime prevention

We will never be able to remove all extremist content online and block all peer-sharing, whether it is encrypted or not, on open or invitation-only closed forums. For some content, it is difficult to prove it is illegal or radicalising, but it is used by agents of radicalisation to lead, to guide in the direction of extremism. Besides, due to the fundamental democratic value of freedom of speech, there will always be disputed material online, which some believe should be removed. In short: there will always be extremist content available, for a longer or shorter period of time.

This is why, besides focusing on extremist content and messengers, it is important to work on the recipient side. We need to make society and vulnerable individuals resilient. This is just another form of crime prevention. These activities should take place in the pre-criminal space – in the field of media literacy, internet safety and online resilient communities with alternative and counter messages. And in this pre-criminal space, police need partners.

Media literacy and online safety are domains where prevention police officers can achieve results with youngsters, their parents and teachers. There is a huge overlap in other risks that require awareness among parents, teachers and others working with youngsters. For instance, recognising propaganda, fake news and conspiracy theories are new skills that are indispensable for youngsters today. Safeguarding against radicalisation and recruitment could be mainstreamed in accepted forms of prevention.

Fighting hate speech and boosting resilience

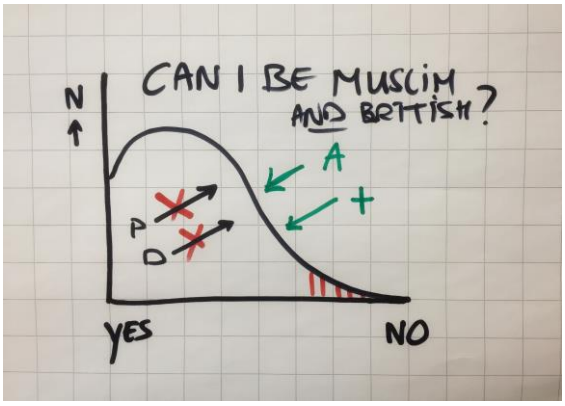
Hate speech covers all forms of expressions that spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance (Council of Europe definition [3]).

Supporting or initiating the fight against hate speech is crime prevention. The German *Helden statt Trolle* (heroes instead of trolls) is an interesting hate speech project. EU-funded, it was initiated by Mecklenburg Vorpommern police in cooperation with a state-supported citizenship institute. The project had both on- and offline dimensions, and aimed at sensitising both police and society to hate speech and fake news by developing and training methods for counter reactions. It thus supported the creation of online and offline communities against hate. Police support for online communities fighting hate speech is the equivalent to police supporting neighbourhoods and shop owners as they seek

[3] https://www.coe.int/en/web/freedom-expression/hate-speech

to create a safer and more resilient environment.

Fighting and countering hate speech supports the powers pushing the bell curve presented below in the desired direction: to the left. We need less propaganda (P) and fewer divisive messages (D) and more alternative (A) and positive messages (+).



An anti-hate speech campaign can mobilise societal resilience and might lead to more referrals for hate speech and the removal of it from online platforms. This has a sanitising effect on the breeding ground, which is being exploited by recruiters and agents of radicalisation.

Working with NGOs

Anti-hate speech programmes are an example of police cooperation with NGOs. The German **Jugendschutz.net** goes one step further. This NGO seeks to protect young Germans from harmful content. This wide definition ensures more options for intervening than offered by legal bodies. And whereas Europol has a mandate only to work on jihadism, Jugendschutz can act against all content that is harmful to young people.

Jugendschutz launched in 2011 with activities against right-wing extremism; jihadism was added later, but before Daesh was well-known. The NGO focuses on general monitoring and targeted research. Individuals can also refer content to Jugendschutz and will have multiple options. There is a hotline to the police, but there are also contact persons at Internet Service Providers and procedures agreed with industry partners. Jugendschutz has a 90% success rate in having content removed after direct contact with the offender. Police and Jugendschutz keep each other posted on operational matters.

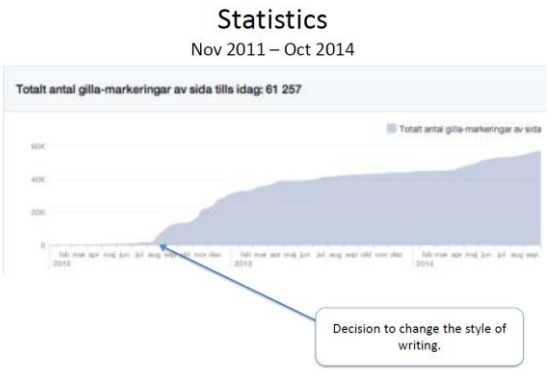
For Jugendschutz it is easier to operate in the grey zone. When is offensive humor officially hate speech? Jugendschutz will pursue content that the police has neither the time nor the mandate to follow up on. There is a large appetite among educators and other practitioners to learn about what happens online. Jugendschutz is a much-appreciated partner for the police in serving the needs of educators and others.

In addition to operations, Jugendschutz also cooperates with the police in research. The cooperation between state monitoring units and this NGO is an inspiring example of how cooperation can have a significant and positive impact on society, leveraging more output.

The police online: communication styles

Just being online will not do the trick for police when they want to engage with the public. In Sweden, a small group of officers was invited to go online and interact with the audience. Initially, they failed to attract an audience. But then they changed something [4].

[4] http://ktar.com/story/228286/swedish-police-to-parents-pick-up-your-drunk-kids/



Several elements can make a real difference. Using attractive pictures and humour can contribute to successful online communication in the competition for eye balls. Messages should also appeal to emotions and be perceived as authentic. Police press messages will not go viral; a committed police officer reproaching parents over their failure to take responsibility will.

Working with industry

The cooperation between, on the one hand police and law enforcement, and on the other hand the internet industry, sometimes resembles a rocky marriage. Neither partner can do without the other, but sometimes they cannot stand each other. In the Oslo meeting, RAN POL learned that Facebook knows even more about users than expected, and that they have their own expertise and CVE staff, more or less like governments and law enforcement agencies have. These mixed teams contain people from different professional backgrounds: for instance NGOs, government and police. Native speakers are included to assess flagged or referred messages because local contexts matter. Facebook has its own apparatus to police and correct its community. In this way, Facebook is trying to get ahead of extremist and other malicious or unwelcome content. The company is able to flag uploaded content and create the equivalent of a digital footprint of it. When it's uploaded again, the machine recognises it and quickly removes it.

Some would say that Facebooks capacities and options even top the possibilities of governments when it comes to monitoring and intervention. This provides more than enough reason to keep pushing cooperation between and with the industry.

Facebook also is better equipped and has more expertise than smaller companies in the business. It would be beneficial to the industry, and society in general, if stronger companies invest in the cooperation among the internet industry parties.

The sharing of information and the cooperation involved in this is not always easy, but can be improved by working with appointed contact persons and agreed protocols.

It takes a network to defeat a network

Extremists master networks and use them for their criminal aims. Engaged supporters help disseminate messages to echo chambers filled with supporters. To be effective against such a network, the police need to mobilise and operate in a network of their own. In NGOs and the education sector, the police can find partners who can help identify unwanted content and even counter it or push for removal. The Internet industry has expertise and access to users.

In engaging with NGOs, the trick is to find common ground and shared goals. We cannot force NGOs to adopt police objectives and support police tasks. Police should present themselves in such a way that they are perceived as partners and allies for NGOs.

Police and moreover governments need to keep pushing the internet industry to take responsibility in this area. That responsibility includes making sure that the facilities they offer are not used to promote extremism or even prepare terrorist acts, and not used to publish material that promotes terror and division.

In preventing and counting online extremism, boosting public-private partnerships with platforms and internet providers can make a real difference.

Key messages

Besides the focus on extremists and their content and activities, police need to contribute to online resilience.

It takes a network to defeat extremist networks. Police need to invest in partnerships with NGOs and the internet industry.

Internet Referral Units, the Norwegian Online Patrolling unit and the Facebook police officers are showing the way in terms of combining online and offline.