

POLICING IN AN ONLINE WORLD

Relevance in
the 21st century



**EUROPEAN
CLEARING BOARD**

Strategic Group
on Online Policing

POLICING IN AN ONLINE WORLD relevance in the 21st century

PDF Web | ISBN 978-92-9414-030-2 | DOI-10.2813/4083983 | QL-01-25-012-EN-N

Neither the European Union Agency for Law Enforcement Cooperation nor any person acting on behalf of the agency is responsible for the use that might be made of the following information.

Luxembourg: Publications Office of the European Union, 2025

© European Union Agency for Law Enforcement Cooperation, 2025

Reproduction is authorised provided the source is acknowledged.

For any use or reproduction of photos or other material that is not under the copyright of the European Union Agency for Law Enforcement Cooperation, permission must be sought directly from the copyright holders.

While best efforts have been made to trace and acknowledge all copyright holders, Europol would like to apologise should there have been any errors or omissions. Please do contact us if you possess any further information relating to the images published or their rights holder.

Cite this publication: *Europol, Policing in an online world - relevance in the 21st century*, Publications Office of the European Union, Luxembourg, 2025.

This publication and more information on Europol are available on the Internet.

www.europol.europa.eu

Policing in an online world - relevance in the 21st century

Presented to the EuCB on 22 March 2024 by the Strategic Group on Online Policing.
Revised in October 2024.

Contents

4	Introduction - It's an online world
	Background
	The challenge – Why online policing?
	21st century policing – Closing the relevance gap
6	Online policing
	Guiding principles of the online police brand
	Online policing – Definition on the basis of the guiding principles
7	Existing initiatives in Europe – Summary
	Norway
	Denmark
	Estonia
	Poland
10	Learning from experience
	Norway
	Denmark
	Estonia
10	The way forward: delivering 21st century services
	Self-assessment
	Human resources, budgets and equipment
12	Appendix A – Existing initiatives in Europe
	Swedish capability model
	Norway
	What is the Danish Online Police Patrol?
	Estonia
20	Appendix B – Supplementary material

INTRODUCTION – IT’S AN ONLINE WORLD

- ▶ In 2023, 92% of EU citizens used the internet¹.
- ▶ The average time – per day – that EU citizens spend online varies between 5 and 8 hours².
- ▶ This is in line with global trends, where the average in late 2023 was around 6.35 hours³.
- ▶ Digital adoption and internet usage accelerated during the COVID-19 pandemic⁴.
- ▶ Young people use online services more often than adults⁵.

Background

The nature of daily life has changed comprehensively in recent years, most notably due to the acceleration of digital adoption during the COVID-19 pandemic, which has led many citizens in Europe to live increasingly digital lives.

Social media, gaming, online banking, shopping or working from home are connecting citizens to virtual communities and online services for up to half of their waking hours (on average).

Digital natives – younger people who grew up in this online culture and are most familiar with it – are spending even more time online.

Criminals have always been quick to exploit technology for their activities. This migration into the digital realm

has resulted in an unprecedented surge in online crime⁶. At the same time, only 54% of EU citizens interacted with public authorities in 2023⁷, of which only a subset involved interaction with the police.

Online worlds are increasingly perceived as lawless spaces that may have profound implications for the safety and security of EU citizens. The safety of individuals and communities are core fundamental human rights⁸, which law enforcement agencies play a crucial role in protecting.

This digital transformation of citizens’ lives demands an urgent response from the police.

The challenge – Why online policing?

As citizens’ lives move increasingly online, the challenge for the police, as the state body tasked with enforcing the rule of law and protecting citizens, is to respond in meaningful ways.

Today, more worlds exist in parallel to the physical realm, as gaming, social media, cryptocurrencies and online marketplaces, among others, create vibrant communities, each with their distinct cultures.

We know that in the physical world, community police officers are an asset in preventing and combating radicalisation⁹. Police may play a direct and indirect role in suicide prevention¹⁰. Public spaces are protected by community policing, which may also play a role in preventing neighbourhood decay¹¹.

When it comes to virtual worlds, such community policing equivalents are often in their infancy or, in many places, simply do not exist. At the same time, physical-world

- 1 Eurostat, December 2024, Digital economy and society statistics - households and individuals, accessible at https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals
- 2 Statista, October 2024, Average daily time spent using the internet by online users in selected countries in Europe as of 2nd quarter 2024, accessible at <https://www.statista.com/statistics/1391355/daily-time-spent-online-europe-by-country/>
- 3 Statista, February 2025, Average daily time spent using the internet by online users worldwide from 3rd quarter 2015 to 3rd quarter 2024, accessible at <https://www.statista.com/statistics/1380282/daily-time-spent-online-global/>
- 4 McKinsey Digital, July 24, 2020, Europe’s digital migration during COVID-19: Getting past the broad trends and averages, accessible at <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/europes-digital-migration-during-covid-19-getting-past-the-broad-trends-and-averages>
- 5 Eurostat, 14 July 2023, 96% of young people in the EU uses the internet daily, accessible at <https://ec.europa.eu/eurostat/en/web/products-eurostat-news/w/ddn-20230714-1>
- 6 Europol, 5 October 2020, COVID-19 sparks upward trend in cybercrime, accessible at <https://www.europol.europa.eu/media-press/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime>
- 7 Eurostat, December 2024, Digital economy and society statistics - households and individuals, accessible at https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals
- 8 Among others, Article 2 (right to life) and Article 5 (right to liberty and security) of the European Convention on Human Rights (ECHR) of 1953.
- 9 European Commission, Radicalisation Awareness Network, 5 August 2021, Conclusions Paper: Community police and the online dimension, accessible at https://home-affairs.ec.europa.eu/system/files/2022-05/ran_pol_community_police_and_the_online_dimension_05072021_en.pdf
- 10 National Library of Medicine, June 2016, Commentary: Police and Suicide Prevention, accessible at <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4896938/>
- 11 National Affairs, Number 63, Spring 2025, Public Spaces in the Digital Age, accessible at <https://nationalaffairs.com/publications/detail/public-spaces-in-the-digital-age>

law-enforcement challenges also exist in virtual communities, and include ensuring the safety and security of citizens (especially minors), as well as fundamental rights, democratic values and consumer protection¹².

If online communities are seen as lawless spaces 'by creating online safe havens of impunity'¹³, ungoverned areas of life will eventually be ruled by the strongest, resulting in the law of the jungle.

The police, therefore, must move into these spaces before they become lawless, in order to protect the rights of citizens and reintroduce the safeguards that underpin life in 21st century Europe.

While the nature and scope of police activities on the internet will vary by country, citizens appear to be positively disposed to such a development.

For example, in the 'Swedes and the internet' report¹⁴, based on a survey that is conducted annually, citizens' attitudes towards online police activities are largely positive.

By way of a second example, a survey of more than 5 500 citizens across 30 countries, conducted by the AP4AI project¹⁵, shows that the vast majority (87% agree or strongly agree) believe that the accountable use of AI by law enforcement is acceptable in certain use cases. This further demonstrates that the use of digital law enforcement activities by the police, where warranted, is acceptable to citizens.

While online policing cannot solve the threat of various types of cybercrime (e.g. malware, fraud) on its own, it will help address community issues relating to citizens interacting with one another in digital spaces.

In a 2021 attitude survey of the Norwegian population, 80% of respondents stated that they had high or very high confidence in the police. However, respondents were not as convinced that the police did a great job when it came to digital crime.

A similar tendency was noted in a 2021 UK survey, which found that only 39% of citizens were confident in law enforcement's ability to protect them from fraud and cybercrime¹⁶.

In the same 2021 survey of the Norwegian population, 93% of respondents felt safe or very safe in the areas of Norway where they travel and live, but only 70% said the same about digital services or online spaces.

In summary, while citizens appear generally positive towards the police engaging in digital law enforcement activities to promote online safety and security, current survey results indicate a capability and relevance gap that the police urgently need to address.

21st century policing – Closing the relevance gap

A modern 21st century police force is a relevant police force.

The police, as a protector of rights in competition with hostile actors seeking to undermine those very rights, must project a values-based narrative that reflects its social contribution in a language that resonates with its citizens and grows with them from youth to adulthood.

Law enforcement has an opportunity to move beyond its current service portfolio in the digital domain to include proactive service offerings based on a set of values that mirror the evolution of society.

By staying ahead of the curve (for example by becoming early adopters of new trends), the police can fend off threats to its relevance.

The internet has had a profound impact on society. It is changing the very landscape of our cities and towns. For example, as banks and post offices close branches, or as traditional department stores lose customers to online shopping equivalents, our physical spaces cede more and more services to their virtual equivalents.

Such changes are not a new phenomenon. Long ago, small corner shops closed due to competition from supermarkets, for example, changing the nature of our urban centres.

What is new is that, for the first time, virtual communities are taking the place of previously physical communities.

12 Council of the European Union, 9 March 2022, Metaverse – Virtual World, Real Challenges, accessible at <https://www.consilium.europa.eu/media/54987/metaverse-paper-9-march-2022.pdf>

13 Council of the European Union, 13 April 2023, Scoping paper for the High-Level Expert Group on access to data for effective law enforcement, accessible at <https://data.consilium.europa.eu/doc/document/ST-8281-2023-INIT/en/pdf>

14 Svenskarna och internet, 10 October 2023, Svenskarna och internet 2023: En årlig studie av svenska folkets internetvanor, accessible at <https://svenskarnaochinternet.se/rapporter/svenskarna-och-internet-2023/english/>

15 Europol, 10 March 2022, New Accountability Framework to use artificial intelligence in a transparent and accountable manner, accessible at <https://www.europol.europa.eu/media-press/newsroom/news/new-accountability-framework-to-use-artificial-intelligence-in-transparent-and-accountable-manner>

16 Ipsos MORI, September 2021, Understanding Society – Crime, accessible at https://www.ipsos.com/sites/default/files/ct/news/documents/2021-09/Understanding%20Society_Crime_Omnibus_Ques_Charting_FINAL.pdf

As a result, the very concept of community policing is struggling with relevance as citizens live first-person lives in physical isolation from one another in order to enjoy virtual connections with like-minded strangers who may be half a world away.

ONLINE POLICING

Guiding principles of the online police brand

A 2023 Swedish study¹⁷ found that police organisations' objectives, aims and goals for online policing were often unclear and varied widely in their approach.

The European Clearing Board's Strategic Group on Online Policing, established in November 2022 and author of this concept paper, brings together law enforcement practitioners from across the EU and from Europol to articulate a set of guiding principles. Based on real-world experience, academic insight and wider societal trends, the group members have synthesised a number of key guiding principles.

For the online police brand to resonate with the changing values of society, to guide its interactions with citizens, and to counter criminal networks spreading into virtual communities, it must:

- ▶ **be permanently present in the online communities where citizens are**, thereby offering safety and protection from online crime as effectively as it does from traditional offline crime, **thus countering the notion that the internet is a lawless space**;
- ▶ **engage with all levels of society at eye level**, from digital natives to digital immigrants¹⁸, by focusing on building relationships through dialogue, **thereby building trust**, especially with hard-to-reach or at-risk target groups;
- ▶ **be transparent**, for example **by being fully uniformed, using police accounts** and declaring its presence and purpose on a digital platform, thereby making it clear that it offers inclusive justice for all segments of society;

- ▶ **stand for evidence-based truth** that is non-negotiable, thereby countering misinformation and fake news **and helping citizens make informed choices when online**;
- ▶ **offer convenience** by lowering the threshold for contacting the police, being available at all times, and making use of online amplification effects, thereby increasing reach.

Online policing – Definition on the basis of the guiding principles

As citizens successfully build more and more of their lives around virtual services on the internet, a permanent police presence must follow them online.

Online policing (also called online patrolling or net patrolling) is typically conducted through visible, uniformed patrolling on digital platforms frequented by citizens, with a specific emphasis on building trust, crime prevention and crime disruption, although it may also involve preliminary investigative case building.

This concept paper recognises that online policing is an emerging area in which law enforcement agencies must engage, while acknowledging that long-established formats of internet-based policing, such as those combating cybercrime, countering online radicalisation and terrorism, and fighting the spread of child sexual exploitation material (CSEM), money laundering and many other types of online crime, are already successfully established.

Moreover, this concept paper acknowledges that online community engagement exists in some form in many LEAs, including police accounts on social media such as Twitter/X or Instagram where citizens can receive up-to-date information or engage with the police in a convenient way.

Since this is an emerging field, we are only now seeing the first scientific studies that help define the concept. A Norwegian study ('Mediated Proximity: Community Policing in the Digital Age'), published in August 2023¹⁹, assesses that:

'(...) online patrols reproduce the core scope of local and community policing in physical spaces, such as local anchoring in a specific community; specific local

17 Eva Jagebo Bonnerud: Online Policing – An Exploratory Analysis searching for guiding principles on Engagement and Interaction with the public, Master's Thesis, Applied Criminology and Police Management, University of Cambridge, 2023

18 Wikipedia, https://en.wikipedia.org/wiki/Digital_native, accessed at: March 2024.

19 Nordic Journal of Studies in Policing, Vol 10 Issue 1, 25 August 2023, Mediated Proximity: Community Policing in the Digital Age, accessible at <https://www.idunn.no/doi/full/10.18261/njsp.10.1.8>, p1.

police tasks such as crime prevention and “everyday offences”; and certain ways of policing locally, for example, via building relations and public trust.’

The definition broadly suggests that online policing can be understood to mean **extending or reimagining the practices of traditional local and community policing in the online realm**.

What this may entail, in terms of concrete tasks, will vary somewhat culturally and regionally. However, the approach taken **must always be transparent, uniformed, active and permanent**.

Additionally, it is important to note that engagement via social media, gaming platforms, chat forums or live events will help **‘to prevent and investigate both online and offline criminal conduct’**²⁰. Online policing is thus not limited to solely dealing with online matters, but provides a contemporary online approach to address crime in its digital/physical hybrid forms.

EXISTING INITIATIVES IN EUROPE – SUMMARY

A small number of European countries have begun online policing activities. The EuCB’s Strategic Group on Online Policing identified a number of permanent initiatives that prominently illustrate the Online Policing concept. This list is not exhaustive and serves as a snapshot in time,

based on the contributions of the 12 countries that are represented in the Strategic Group.

Norway

The National Criminal Investigation Service (NCIS) of Norway has been present online since November 2015, when the police established an online police presence by creating a Facebook page.

The first police districts established their own online patrols in 2018 and, since 2020, all 12 districts have had their own online patrol (nettpatrolje). In 2023, approximately 45 police employees in Norway are tasked with online policing duties. Until 2025, the NCIS had the responsibility of coordinating the online patrols and working to develop new methods that are suitable for the Norwegian police’s online presence. Currently, the online patrols are visibly present and communicatively available for citizens on social media platforms. Additionally, they conduct investigatory police work online.

A vast majority of the Norwegian population use social media on a daily basis ²¹, and it is thus highly important that the police are present in these online venues. The main aims of the uniformed online presence are to:

- ▶ prevent crime,
- ▶ contribute to online safety, and
- ▶ bolster trust in the police.



Nilsen, NCIS Norway “The Norwegian police patrolling the Internet”.

20 Nordic Journal of Studies in Policing, Vol 10 Issue 1, 25 August 2023, Mediated Proximity: Community Policing in the Digital Age, accessible at <https://www.idunn.no/doi/full/10.18261/njsp.10.1.8>, p2.

21 Ipsos, 31 October 2023, Ipsos SoMe-Tracker Q3’23, accessible at <https://www.ipsos.com/nb-no/ipsos-some-tracker-q323>

The regional online patrols cooperate with local police officers and constitute a district-wide resource in matters related to online policing, contact with platform owners, as well as searching for and collecting evidence on social media platforms.

Some of the online patrols also engage in online gaming with children and young people as part of their online patrolling practices. This is especially aimed at engaging with hard-to-reach or at-risk young people on their own terms and on digital platforms they are comfortable with. Gaming as a method of community policing is highly flexible and includes opportunities to reach out broadly to citizens in general (primary prevention) or to focus on specific target groups (secondary and tertiary prevention).

Denmark

The Danish Online Police Patrol works with various aspects of online policing. The unit includes 10 people (seven police officers, one civilian analyst, one communications expert and a head of unit) They operate on various platforms with different targets and audiences. The main point of online policing is to show the police's presence and to enhance safety where citizens are.

The Online Patrol works on prevention at different levels, depending on the target groups. It is active on different social media platforms, also determined by the target group. However, since children and young people are especially active on gaming platforms, the Online Patrol also engages in gaming as a way to interact with them.

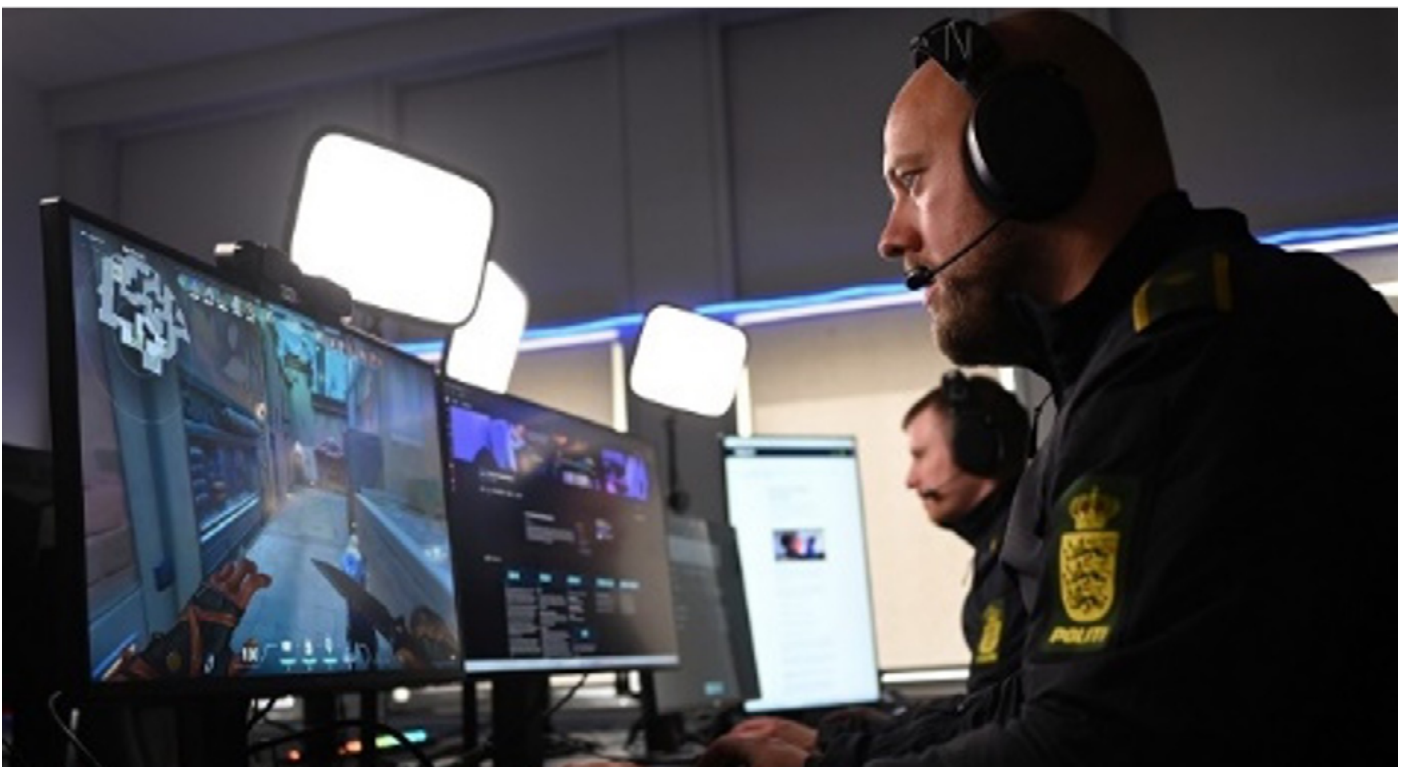
The Online Patrol uses various games to reach different audiences based on their age. For instance, to play with the youngest children, the Online Patrol uses Roblox and Minecraft. To reach an older audience, the games played are Counter-Strike and Fortnite.

Gaming is usually livestreamed through Twitch, which reaches a larger audience than the few children actually playing at the time. This creates opportunities for interactions with thousands of people through a few hours of gaming.



"Keyboard from the Danish online patrol", SOURCE: Danish Police

The Danish Police use open-source intelligence (OSINT) to investigate online crime. Citizens can contact the Online Patrol on various platforms regarding suspicious activities or with tip-offs. The Online Patrol makes much use of OSINT to narrow down a field of possible perpetrators or to find out more information to shed light on a case. The Online Patrol is a specialised unit that is expanding the number of areas in which it works.



"Members of the Danish online patrol livestreaming on Twitch", SOURCE: Danish Police

The Online Patrol tries to stay ahead of new trends or tools on the internet that might create issues for the police later on. They cooperate with Europol on work regarding the metaverse, virtual reality and augmented reality.

For the Danish Police, online policing involves a combination of prevention, disruption and investigation activities on online platforms.

Online policing involves preventing, disrupting and investigating crimes that take place in the online sphere. The Online Patrol has had a couple of noteworthy results in its first two years of operations. This increases people's trust in the police, which also makes them more likely to contact the police. The fact that the cost of creating and operating an online patrol is less or equivalent to that of a patrol vehicle should encourage most countries to start up a unit.

Estonia

In Estonia, the concept of online policing is known as 'Virtual Community Policing' (VCP).

The Estonian Police and Border Guard Board (PBGB) initiated VCP in 2011 with one police officer. The aim was to provide the same service as community police provide in the real world, but in virtual environments. It quickly became clear that the public liked using this easy way to contact the police, as they used this channel to ask for advice, express their concerns, send tips about possible crimes and so on.

In 2022, the initiative took a new turn and instead of three VCP officers, there are now 13, with plans to expand the team even further.

A VCP officer works on social media with a personalised account, using the officer's real name and photo. This means that people know exactly whom they are talking to. VCP works on most of the main social media platforms that citizens tend to use. The intention is that VCP becomes an integral part of online communities so that a partnership based on trust can be formed between the police and the people of Estonia.

Poland

The Polish Police consists of the National Police Headquarters, 18 provincial headquarters (including the Metropolitan Police Headquarters in Warsaw with the rights of a voivodeship command), city, county and district headquarters, and police stations.

Additionally, there is the Central Bureau of Investigation (CBol), which deals with combating organised crime,

the Central Cybercrime Bureau (CCB), which deals with fighting crime on the internet, the Central Police Forensic Laboratory and the Police Academy, and also police schools.

All the entities mentioned above maintain separate websites and they use the National Police HQ's social media to a greater or lesser extent.

The National Police Headquarters, CBol and CCB publish information on the internet that is relevant for the entire country. The Polish Police maintains accounts on social media such as Facebook, X, LinkedIn, YouTube, Instagram, Tik Tok and Threads.

In Poland, online policing activities mainly consist of:

- ▶ maintaining the National Police websites;
- ▶ maintaining accounts set up on social media such as Facebook, Twitter/X, LinkedIn, YouTube, Instagram, TikTok, and Threads;
- ▶ organising and participating in online webinars with the possibility of interacting with the public (e.g. asking questions);
- ▶ preparing press releases and information material;
- ▶ participating in conferences and training conducted via the internet;
- ▶ appearing regularly on television programmes and radio broadcasts on national and local stations;
- ▶ participating in webinars with national institutions in the field of cyber hygiene.

The Central Cybercrime Bureau (CCB) also monitors the network for:

- ▶ disclosing threats related to public safety and order;
- ▶ recognising new methods and trends in the activities of perpetrators of crimes committed using an IT system, ICT system, ICT network;
- ▶ hate speech.

In justified cases, the CCB performs activities related to OSINT. The CCB has a 24/7 division that operates continually. This division's responsibilities include activities related to threats to the life and health of citizens, and terrorist threats, such as searching through information on the internet related to the planting of an explosive device.

An email address is provided by all police units, as well as on the Public Information Bulletin website, to which every citizen can submit an application for access to public information or send information to the Police.

LEARNING FROM EXPERIENCE

Looking at these pioneer initiatives, significant findings can be articulated even after only a relatively short space of time.

Norway

Norway has chosen a decentralised model with regional online patrols to promote close proximity to the public, as many citizens feel closely connected to their local online patrol operators. The organisation provides a close cooperation between the online patrol and other units within the police district. **The decentralised organisation also provides the police with the opportunity to reach out locally to citizens with custom content covering topics that are of especial relevance within the geographical area of the district.** While the online patrols are comprised of relatively few employees and are not staffed around the clock, other units in the police district help to monitor the messages received when the online patrol is unable to do so. In this way, the public can receive answers at any time of the day, and time-critical messages are followed up on instantly.

To organise Norway's decentralised model, national coordination becomes important. The National Cybercrime Centre (NC3) at the NCIS had overarching responsibility for the field of online policing methods during the establishment phase until 2025, and coordinated the online patrols. This involved coordinating the 12 online patrols, arranging regular meetings, ensuring that employees develop the necessary skills/competences and working on method development.

The experience of the **online patrols is that their online presence and patrolling is well received by the public.** Since the Norwegian police have been online for many years, the population is also accustomed to such presence. Through their experience, the online patrols have developed in-depth knowledge of the different social media platforms, and thus are capable of adjusting to different digital ecosystems and online cultures in order to fully participate and conduct their online policing duties.

Denmark

In Denmark, a measurable improvement in the perception of the police can be attributed to their online engagement. Their online presence presents a human face to online citizens. The perception of a safe space online driven by police engagement there allows a contrasting and much more positive narrative to emerge.

The internet is not a lawless space!

Speaking to children and youngsters at eye-level, listening to them, and taking them seriously have all had a positive impact on the perception of the police and the public's trust in them. Enquiries about online security have risen.

There are growing numbers of tip-offs and gaming-related reports of criminal behaviour. Collaboration with administrators and moderators is helping build trust. Hard-to-reach communities are now within reach.

Estonia

As VCP, officers are active members of their online communities, they participate in different groups and chats, A VCP officer is a credible voice within communities. A VCP officer represents a trustable person to turn to if you are in trouble and would like consult someone who does not take sides, but helps you find a way to begin dealing with your issues. VCP officers often reach out to persons who have been reported missing, in order to make contact with them, talk to them if needed, and get information from them to make sure they are OK. We have even had cases where a VCP officer took the role of negotiator with a suicidal person, keeping her active in a chat until help arrived on the scene.

THE WAY FORWARD: DELIVERING 21ST CENTURY SERVICES

In response to societal change, the police must change too.

The concept of online community policing represents a low-cost/high-impact method of modernising the service portfolio of the police.

As the examples provided illustrate, the initial service offering may be modest in scope, but from an initial pilot involving only a few police officers, it could grow into an entirely new and relevant police service portfolio.

When assessing a Member State's readiness to move to online policing, a number of parameters must fall into place, not least the legal framework to permit law enforcement activities such as those described in this document.

See Appendix A for a self-assessment capability model developed by the Swedish Police.

Self-assessment

Assuming the need for online policing is recognised and accepted, an implementation plan may be developed with relative ease. The principal assessment to make is whether existing laws permit the police to be present in online worlds.

If they do, using the Swedish capability model allows an implementing police force to examine readiness from multiple angles using simple red-amber-green traffic light colouring. If too many of the domains under assessment are red or amber, fine-tuning or lowering the scope may turn those domains green, thereby better predicting what a first pilot project might look like.

Similarly, if the initial scope shows an all-green self-assessment, it may be worth considering a more ambitious approach to make the pilot project more impactful.

Human resources, budgets and equipment

As indicated above, experience shows that an initial project of modest size and scope may already have a substantial impact.

A pilot project may only require a small number of police officers to begin with. Ideally, these officers will be digitally literate and have social media and/or gaming experience.

The cost of starting an online patrol may be lower than the cost of a squad car.

Adding a social media manager and a technically proficient camera operator/editor (who may be a civilian) will allow for recognition of current trends, careful planning of online campaigns and the production of quality content.

Depending on the scope of the initial pilot project, the investment will also be modest, requiring some specific equipment (for example headsets, gaming PCs, cameras and editing software, online subscriptions for certain platforms), but not needing specialised back-end enterprise-grade solutions.

APPENDIX A – EXISTING INITIATIVES IN EUROPE

1. Swedish capability model

The Swedish Police have developed a capability model using four key domains on which a self-assessment can be performed regarding the police's readiness for online policing.

A capability in this context refers to the ability to perform a desired activity or action independently at a desired time and without limiting factors. A capability must be able to create value in any given operation and in any given situation. In order for a capability to exist, specific conditions must be met and the necessary capacity must be there.

The domains are:

1. The operational domain, for example laws and regulations, or internal guidelines that define the framework for how the capability is to be managed and, to the extent necessary, how it is to be regulated.
2. The system-based domain, which includes IT systems, premises/vehicles and equipment needed to perform the capability.
3. Structural domain, for example resources (including budgets), leadership or external factors that define the mutual relationships or the context

that exists between the parts of a whole and the capability itself.

4. Competence-based domain, such as the knowledge, attitudes or skills that are needed to execute the capability.

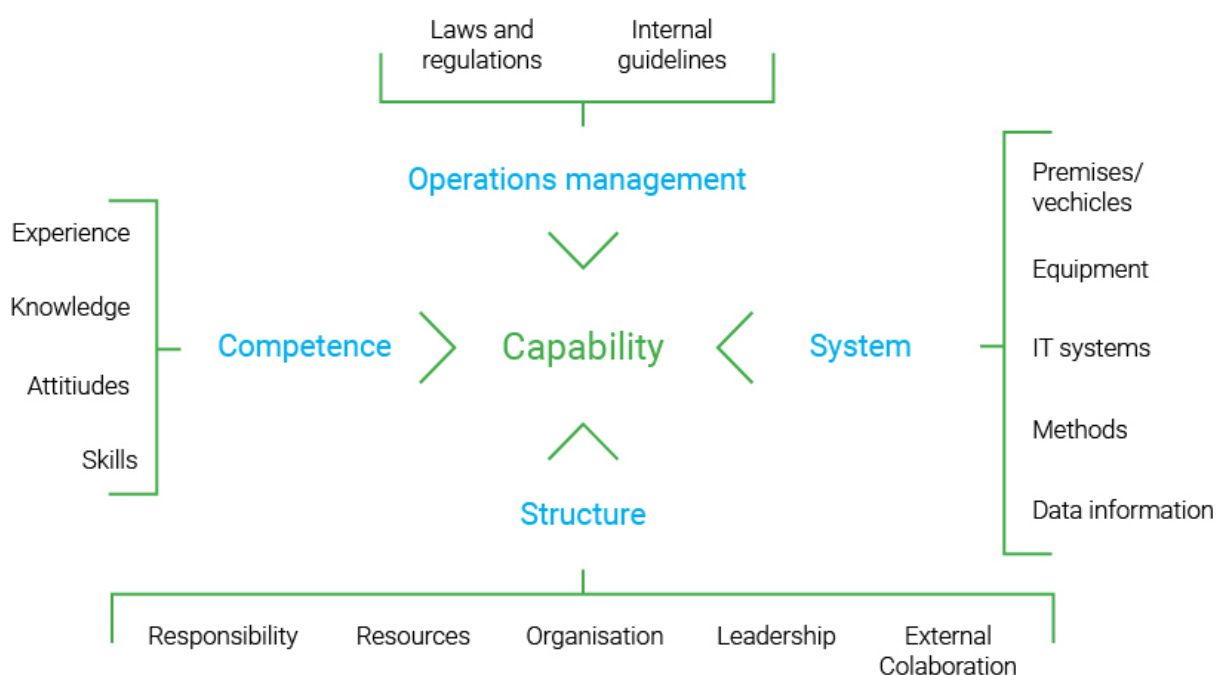
Defining an online policing competency and then using the capability model to self-assess the police's readiness represents a first step on a roadmap to offer relevant 21st century services to citizens.

2. Norway

The National Criminal Investigation Service (NCIS) of Norway has been present online since November 2015, when the police established an online police presence by creating a Facebook page.

The first police districts established their own online patrols in 2018 and, since 2020, all 12 districts have had their own online patrol (nettpatrolje). In 2023, approximately 45 police employees in Norway are tasked with online policing duties. The NCIS has the responsibility of coordinating the online patrols and working to develop new methods that are suitable for the Norwegian police's online presence. The online patrols are visibly present and communicatively available for citizens on social media platforms. Additionally, they conduct investigatory police work online.

A vast majority of the Norwegian population use social media on a daily basis, and it is thus highly important that the police are present in these venues.



The main aims of the uniformed online presence are to:

- ▶ prevent crime,
- ▶ contribute to online safety, and
- ▶ bolster trust in the police.

The regional online patrols cooperate with local police officers and constitute a district-wide resource in matters related to online policing, contact with platform owners, as well as searching and collecting evidence on social media platforms.

Online policing in Norway consists of both an open online presence and online patrolling activities. The first of these approaches comprises the use of uniformed social media accounts to publish public messages and to engage in dialogue by responding to comments and direct messages. The posts that are published revolve around both online and offline matters, and include preventive messages, glimpses into everyday police work, warnings, advice and guidance. This allows the police to reach out rapidly to thousands of citizens with important public service messages. Broadly speaking, an online presence involves societal participation on the internet, to show that the police care about what happens online and to actively maintain dialogue with the public. Through public posts and dialogue, the police can contribute to preventing 'fake news' and provide nuanced information on various topics. In 2023, the online patrols have accounts on Facebook, Instagram, Snapchat, TikTok and YouTube.

The online patrols receive direct messages through Messenger and Instagram. Many, especially young people, are more comfortable contacting the police via messaging services rather than calling over the phone. Thus, the online patrols are available to receive direct messages through Messenger and Instagram, which are among the most popular platforms for direct messaging in Norway. The online patrols have received approximately 2 500 direct messages every month in 2023. Messages typically revolve around topics such as bullying, image sharing, tips about accounts used for illicit activities, dangerous 'challenges', videos documenting violence, and hate speech.

By being approachable online, the online patrols receive information that the police most likely would not have become aware of otherwise.

The second approach, namely online patrolling, is when police officers actively seek out social media platforms to participate in those communities, rather than broadcast messages within the channel or page established by the police.

Online patrolling is thus about participating on an equal footing with other users and engaging in ongoing online discourse.

Practically speaking, this involves joining groups, servers, channels or forums on social media platforms and participating with uniformed user profiles. This provides a great opportunity to improve dialogue with the public and to increase trust in the police. Additionally, it serves an important purpose of disseminating important preventive messages to target groups who may otherwise be hard to reach through top-down communication. Lastly, the online patrols may provide added value to online discussions by countering misinformation. The Norwegian police has actively patrolled Discord, Reddit, Omegle and Telegram, as well as Facebook groups with a local scope.

Some of the online patrols also engage in gaming with children and young people as part of their online patrolling practices. This is especially aimed at meeting the target group in their very own arena, and the conversations are typically free-flowing between game-specific matters and everyday life. Gaming as a method of community policing is highly flexibly and includes opportunities to reach out broadly to citizens in general (primary prevention) or to focus on specific target groups (secondary and tertiary prevention).

Online patrolling on gaming platforms can increase young people's perceived online safety, contribute to combatting 'toxic' communication and demonstrate that the internet is not a lawless space. The Norwegian police have so far patrolled Minecraft, Roblox, FIFA, Fortnite, League of Legends and Counter-Strike. In addition, it is important to note that some sessions are live-streamed on Twitch, which greatly increases the reach of the method.

The online patrols regularly arrange digital parents' meetings that reach out to thousands of parents and guardians. Some of these meetings are publicly available through direct streaming on Facebook and YouTube, while others are invite-only or target a specific geographical area. Viewers can pose questions directly in the chat and receive responses throughout the digital meeting. Another advantage of digital parents' meetings is the opportunity to share recordings online. The addition of subtitles in other languages further improves the potential reach of such meetings.

3. What is the Danish Online Police Patrol?

The Danish Online Police Patrol works with various aspects of online policing. It works from an intelligence-led policing (ILP) principle to make the most of a small unit.

The unit includes 10 people (seven police officers, one civilian analyst, one communications expert and a head of unit). They operate on various platforms with different targets and audiences. The main point of policing online is to show presence and enhance safety where citizens are. The police should be reachable both offline and online, and the Danish police wanted to create a digital unit whose purpose was to prevent, investigate and disrupt online crime.

This gave rise to the Danish Online Police Patrol (henceforth, 'Online Patrol'). From a Danish point of view, online policing is like physical police work, only in an online sphere. This means that just as the police patrol the streets, they should patrol the internet. The same goes for preventative measures, investigations and so forth. The following sections will dive into the different aspects of online policing in Denmark, how it is done, and what the focus is in each of the different areas.

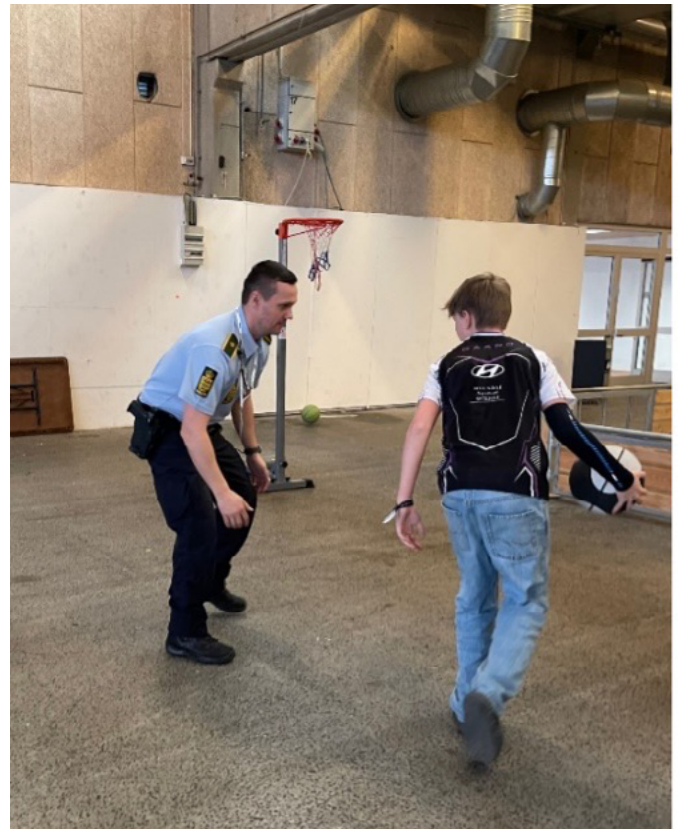


Members of the Danish online patrol on a stage in Herning, Denmark

One of the first tasks of online policing is to make sure that the public knows they are communicating with the police and not with fraudulent users. It is important for an online policing unit to have usernames, profile pictures, cover pictures and other noticeable features on all their profiles, so that the public recognises the unit as the police. At the same time, it is a good idea to verify the various profiles used on platforms/social media and to verify the profiles on the police's own website. This reduces the risk of citizens being fooled by fake accounts, and makes it easier

to strike down accounts pretending to be the police and prosecute those behind them.

It should always be clear that content posted from police accounts comes from the police and it should therefore fit with a certain image. This is one of the reasons why having officers in uniform in videos or images makes sense. Officers in an online policing unit might become recognisable to the public, because they will feature in a lot of content; this is a benefit for the unit, because it instils trust in the public's view of the police and increases their willingness to contact the Online Patrol.



A member of the Danish online patrol playing basketball with a child at a gaming event

An online policing unit has to be present on some of the most popular social media platforms in the given country. However, even if a specific platform is not going to be used imminently, it is a good idea to secure an account with a similar name structure on all possible social media and gaming platforms to further minimise the risk of trolling or fraudulent behaviour.

PREVENTION

The Online Patrol works with prevention on different levels, depending on the target groups, and is active on different social media platforms, also determined by the target group. This is to make sure that the target group receives the correct messages and is not exposed to unnecessary information from the Online Patrol. Targeting groups ensures that the unit reaches the intended audience

intelligently and successfully and that the effort is well received on the various social media and online platforms.

Social media

To reach the youngest audience on social media, the Online Patrol is active on TikTok and YouTube. To reach an older audience, it is active on Instagram and Facebook. The Online Patrol reaches gamers by being active on Discord and Twitch, among others. The list of social media changes depending on where the target group operates and what the intention of the Online Patrol is. This means that the Online Patrol must have fluid work processes and it also demands a broad understanding of the internet, various forums, social media and gaming platforms.



Members of the Danish online patrol talking to children and youngsters at a gaming event

Content on the platforms must also appeal to the audience, so the Online Patrol has to operate with credibility on the particular platform. This means that a video created for TikTok might not be published on other platforms, as it would not create the desired response, either because of the content or because of the audience's behaviour on the platform. It is important that content on the platforms is at eye level with the audience and shows the police from a nuanced point of view in order to best connect with the public.

By being at eye level, the Online Patrol shows the police as human beings, using a language the particular target group understands and appreciates.

This applies to all the content posted.

If the desired response is fun interaction with young people, the video produced must have some element of humour in it.

If the desired response is for older people not to be scammed, the pictures must be highlighted in a way that catches the eye, while giving a clear-cut message, with only a few tips on how to behave in this regard.

Humorous content is not only used as entertainment for the user; it is also used to draw users into watching other content on the platform, so that they receive information on important matters.

Gaming

The Online Patrol uses gaming as an interactive form of connecting with young people. The idea behind this is the same as that of community police playing football at a youth club, which is to give young people a better understanding of and respect for the police, and to create unique moments with positive memories regarding the police.

It helps young people gain trust in the police, so that they will hopefully contact them when and if they need them. It also creates a lot of room for conversations in which questions regarding anything and everything can be answered, the purpose being to make the children involved in gaming aware of important issues.

The gaming community represents a large portion of the public, made up of people who spend a vast amount of time on the internet every day. They are therefore likely to stumble upon something of interest to the police. This makes this specific target group extremely important for the police to try to reach, especially given that it is a group that has been overlooked for a long time.

The Online Patrol also makes contact with administrators and moderators in different gaming communities in order to explain their presence and to spread their messages to their specific user base. The Online Patrol uses different games to reach different audiences, based on their age. For instance, to play with the youngest children, the Online Patrol uses Roblox and Minecraft. With older audiences, the games played are Counter-Strike and Fortnite. The games are usually livestreamed through Twitch, which takes it to a larger audience than only the few children actually playing at the time. That creates opportunities for interactions with thousands of people through a few hours of gaming. Because of the sizes of the audience, livestreams are also used for general Q&As or to dive in to a topic of interest for the police.

Partners and events

The Online Patrol makes a great effort to be in touch with the relevant stakeholders in Denmark and internationally. Nationally, the Online Patrol works with multiple partners to prevent online crime.

These partners include NGOs such as Save The Children Denmark and the Danish organisation Børns Vilkår (Children's Rights). It also includes external authorities, such as municipalities and their radicalisation or youth crime prevention teams. Within the Danish police, the Online Patrol works together with the Danish Intelligence and Security Service (PET) and with the National Cyber Crime Centre (NC3).

Other partners to mention are the Centre for Cyber Security in the Danish Defence Intelligence Service (FE) and the Centre for Digital Youth Care under the Ministry for Digitisation, as well as international partners, such as Europol.

It is important for the Online Patrol to attend events all over Denmark in order to meet citizens in person, to raise awareness of the Online Patrol's messages and to address large audiences on the common theme of online security. The Online Patrol puts a lot of effort into making sure people of interest know about them. This is why – as experts on the subject of children's use of online platforms, prevention of online crime, social media and more – the Online Patrol spends a significant amount of time giving lectures to people of interest regarding how the Online Patrol works, use of social media and how to prevent different kinds of crimes online.

Other preventative measures

To tackle emerging trends head on, the Online Patrol sets up online meetings for children or parents, depending on the topic. The idea is for the police to invite subject matter experts on a current trend talking about that trend from their point of view, while the Online Patrol gives the police's point of view and advice on the subject. The objective is to have as nuanced a discussion as possible, in which viewers have the opportunity to write questions about the subject directly on the screen. These meetings have taken place on Facebook Live, but could also be on YouTube, Twitch or another streaming service.

INVESTIGATION

Because citizens in Denmark have several platforms at their disposal through which they can contact the Online Patrol regarding suspicious activities or with tip-offs regarding online crime, the Online Patrol can set up investigations.

The Online Patrol primarily uses open-source intelligence (OSINT) in its investigations because of the nature of the tip-offs received. Usually, the tip-offs focus on a group of people or a specific account on a specific social media or gaming platform.



Members of the Danish online patrol awarding a "Danish Game Award" for "Family Friendly Gamer of the Year."

This immediately creates an issue because users often choose usernames that are semi-anonymous. The online patrol makes great use of OSINT to narrow down a field of possible perpetrators or to find out more information to shed light on a case.

The nature of the tip-offs and inquiries gives the Online Patrol insight into current trends, which they use to determine which cases to look into more closely, and which cases to forward on to the police districts. These inquiries are also a great way to help citizens improve their reports to the police. By giving the public the correct links to report the crimes, informing them about potentially critical evidence that might disappear or anything else of relevance to a case, the Online Patrol creates better case files from the outset. Conversations are also used to give citizens an understanding of what crimes, if any, have been committed. The Online Patrol also guides citizens to other types of help if it is not a police matter or if someone other than the police can provide better assistance.

There have already been many instances of the Online Patrol investigating crimes which the police might not otherwise have found out about. One example is a case situated in a gaming community. Because of the in-game ranking system, a specific individual had a huge amount of power over the other players. He used this power to make young boys send pictures and videos of themselves wearing little to no clothing, so that they could rise through the ranks in the game.

The Online Patrol heard of this grooming activity from bystanders who had witnessed something odd about the perpetrator's interactions with other players and contacted

the Online Patrol because of this. This individual was sentenced for violating the Danish penal code.

Cooperation with police districts

Because the Online Patrol is a national unit, it relies heavily on the continued cooperation with police districts in Denmark, Greenland and the Faroe Islands.



Members of the Danish online patrol gaming with children at a gaming event.

When the Online Patrol investigates a crime, the case ends up in a police district, so it is important that the Online Patrol creates a solid and well-evidenced case before sending it to the district. Because of the influx of tip-offs and general patrolling of the internet, the Online Patrol comes across many potential cases to look at. It is important to take the time to talk to the citizens contacting the Online Patrol, reviewing their tip-offs or guiding them on reporting it.

This creates confidence where the police districts can be sure that the cases coming from the Online Patrol are of importance. At the same time, the Online Patrol is dependent on the police districts for day-to-day police work such as arresting perpetrators, carrying out inquiries (for example, the Online Patrol has received several reports concerning children at risk of suicide, requiring collaboration with the police district in terms of physical contact and providing help to the child) and so on, which gives the Online Patrol a strong incentive to create solid

cases for the police districts to pursue. It also increases the quality of reports from citizens, as the Online Patrol guides and informs them on which evidence they need to secure and include.

Expertise

The Online Patrol is a specialised unit which is continuing to grow the areas it works in and is still gaining knowledge about different aspects of the internet. The Online Patrol tries to be ahead of new trends or tools on the internet that might create issues for the police later on. This is why it cooperates with Europol on work with the metaverse, virtual reality and augmented reality.

The Online Patrol looks at artificial intelligence and how to use it in investigations or how criminals might use it. It has created a number of court-ready reports on social media for the police districts to use when they have a case where a specific social network is involved. Because the internet is an ever-growing part of everyday life, it is important for the Online Patrol to continue to try to stay ahead of all possible trends and issues.

DISRUPTION

The Online Patrol acknowledges that it is impossible to prevent or investigate every crime online, which is why they also put a large amount of effort into disrupting crime. Much of this effort focuses on how to better target different types of crimes online, but there are examples where disruption can be effectively applied.

For instance, if the Online Patrol finds a group on Facebook that is predominantly used for selling illicit substances, the Online Patrol will cooperate with the Danish Single Point of Contact (SPOC), who has the contact to the platforms, to take down the Facebook group. This will make it more difficult for these crimes to continue, given that the sellers will have to rebuild their marketplaces again.

Disruption can also be used as a tool in more anonymous areas of the internet. For example, on Telegram, the user base might think that they are anonymous, but there have been examples of the Online Patrol finding specific perpetrators of distribution of child sexual exploitation material (CSEM). Once the perpetrators had been caught and charged, the Online Patrol posted on the multiple Telegram groups that an operation had taken place and that many people on these Telegram groups were being charged for their crimes. This scare tactic worked, because there was both a departure of users in the groups and a drastic fall in the sharing of CSEM and revenge pornography.



Member of the Danish online patrol at a gaming event.

A significant part of the daily work of the Danish Online Patrol involves disrupting criminal activities across various online forums and platforms, where they engage with the public. Such patrolling can be compared to the police patrolling offline communities and high-risk areas in a patrol car.

Targeted patrols

Another way of disrupting online crime is through what the Online Patrol calls targeted patrols. The idea is that the targeted patrols are based on police intelligence, tip-offs and a general understanding of which areas of the internet to target, in order to demonstrate police presence most effectively.

For instance, if the Online Patrol gains knowledge of a particular area of the internet where a criminal activity is occurring, it can actively engage in conversations through public profiles to interrupt the crime. This will discourage the perpetrators from being there and disperse them from the platform. Although this might lead to the perpetrators moving to other, more strongly encrypted, messaging services, making it harder to investigate them, it also creates a smaller buyer base since they are using less commonly used media to commit their crimes, thereby removing their presence from the public's view.

Targeted patrols can also be used to reach a particular audience, where the goal is not to disrupt crime but to inform groups about online safety or how to behave in relation to a current trend or bigger national event. This represents a more operative way of trying to connect to young people and giving them information relevant to the current situation.



Member of the Danish online patrol talking to citizens at a gaming event.

It is an example of how one tool can be used either to disrupt crime or to prevent possible victims from being targeted by the criminals. One concrete example might be the Online Patrol being active on a Subreddit, where a topic of interest to the police is being discussed; the Online Patrol can engage in the conversation and clarify matters that might be based on a wrong assumption or help a user who is struggling mentally and might be suicidal.

FINAL THOUGHTS

Online policing, like conventional policing, involves preventing, disrupting and investigating crimes, the difference being that these crimes take place in the online sphere. To make it a success, it is important that the officers working on these areas work well together. Expertise is essential; if the Online Patrol did not have the expertise needed for carrying out the many different aspects of police work online, it would not succeed. By effectively working with the different aspects of online policing in-house, timewasting and unnecessary bureaucracy are reduced.

Young people are more likely to listen to their favourite influencer on matters that are important to them rather than conventional news media. By making police officers influencers, the opportunity to influence young people in a positive direction arises.

Preventative work, such as engaging in gaming with young people or posting humorous content on social media,

creates relationships with the public. This increases people's trust in the police, which also makes them more likely to contact them. Tip-offs might lead to introducing a targeted patrol into a specific online community, which in turn could lead to knowledge about a specific user that requires the Online Patrol to investigate further or that creates a way to disrupt the criminal network.



Member of the Danish online patrol playing Tekken on Playstation with children.

Investigations provide a better understanding of the criminal activity in general and might lead to new preventative measures, and thus the loop is closed between prevention, patrolling and investigation.

The fact that the cost of creating and operating an online patrol is less than or equivalent to that of a patrol vehicle should encourage most countries to start up a unit and try it themselves. In the end, the question is whether we can really afford for the internet to be a lawless space or, perhaps even worse, for only third parties in the tech industry to be policing it.

The Online Patrol has had a couple of noticeable results in its first three years. It has more than 630 000 followers on TikTok, 30 000 followers on Twitch, 20 000 followers on Facebook, 40 000 followers on Instagram, and 5 000 followers on their Discord server. Its content has received millions of views on TikTok and elsewhere. More than 200 000 unique users have seen its livestreams on Twitch.

All of this is great exposure for the police in general, creates a better public opinion of the police and reassuring the public of the police's ability to help them. More interestingly, this exposure creates more awareness of the Online Patrol in Denmark, making citizens more likely to contact the police when they need help online.

Giving citizens new ways of contacting the police ensures that the police stay relevant. This is especially true for young people, who are much less inclined to call the police. Young people tend to use more unconventional ways of communicating, like chatting online. This is clear from the fact that more than 10 000 unique users have chatted with the Online Patrol on Discord, Messenger and Instagram Direct.

In addition to preventative measures such as videos and unique chats, the Online Patrol has also helped in several cases, including some highly political cases and some cases covered by the mass media. These include the shooting in the Field's shopping centre, big grooming cases and the removal of CSEM, revenge porn and terrorist-related videos online.

The Online Patrol was very aware of the fact that some people might criticise the police for being on various social media and gaming platforms, because it might not be immediately obvious to the broader public why the police should be present in these areas of the internet. To counter this possible criticism, the Online Patrol made sure to answer comments as professionally and methodically as possible. This meant that the number of comments regarding the use of taxpayer money or similar went down substantially and quickly.

Ultimately, online policing has almost endless possibilities, and while some things work in Denmark, they might not work the same way in another country. Depending on the online demographic in various countries, some platforms might be bigger or smaller and therefore more or less interesting to work on from the police's point of view. The same goes for different gaming communities; in one country a specific game might be extremely popular and in another it might be niche. There is therefore no formula for every country to go by, but some of the Danish Online Police Patrol's ideas can certainly be used in other countries looking to start an online patrol.

4. Estonia

In Estonia, the concept of online policing is known as 'Virtual Community Policing' (VCP).

The Estonian Police and Border Guard Board (PBGB) initiated VCP back in 2011 with one police officer. The aim was to provide the same service as community police

provide in the real world, but in virtual environments. It quickly became clear that the public liked using this easy way to contact the police, as they used this channel to ask for advice, express their concerns, send tips about possible crimes and so on.

In 2022, the initiative took a new turn and instead of three VCP officers there are now 13, with plans to expand the team even further.

A VCP officer works on social media with a personalised account, using the officer's real name and photo. This means that people know exactly whom they are talking to. VCP works on most of the main social media platforms that citizens tend to use. The intention is that VCP becomes an integral part of online communities so that a partnership based on trust can be formed between the police and people of Estonia.

In 2023, the VCP team responded to almost 12 000 different requests. A vast amount of these were citizens notifying the PBGB about different scams. This information is then used to publish posts on our accounts warning people about these scams.

It is important to note here that VCP does not initiate or carry out investigations; VCP officers collect the information that is provided and send it to investigative units. VCP officers also support investigations on data gathering and reach out to users when more information is needed.

In VCP, voluntary police officers also play a big role, helping us find troublesome content and reporting it to platforms for deletion. In 2023, there is a group of 21 volunteers, each of whom contributes about two to three hours per month to support our goals.

APPENDIX B – SUPPLEMENTARY MATERIAL

Video – Kripos Norway – Online Policing

<https://www.youtube.com/watch?v=75tNpSHfLeI>

Video – Danish Online Police – Because Denmark is Online (Danish with English subtitles)

<https://www.youtube.com/watch?v=-7UKoP7VP28>

