TERRORISTS’ USE OF THE INTERNET AND THE CHALLENGES COMING OUT OF COVID.
The Covid-19 pandemic has been a seismic global event that has caused devastating social and economic disruption, impacting communities and individuals across Europe. As a result, the pandemic has brought about a rapid pace of change, both to the way that we live and the way that we work. Perhaps most noticeably, and significantly, it has instigated an unprecedented digital transformation.

This digital transformation has shaped the way in which we all interact and socialise with one another and given new opportunities for how we do our work. The last year has seen the adoption, en masse, of new digital technologies. Whilst these technologies have enabled us to keep in touch with one another, to work and to be entertained, they have also presented a new set of challenges.

These technologies have given terrorists and extremists, who are often pioneers and innovators in the digital space, new opportunities to adopt and adapt them to radicalise and recruit. Most notably, in Europe, people have observed the recent digital recruitment tactics of violent right wing extremist (VRWE) groups.

Not only are people accessing more extremist content online, including conspiracy narratives, but they can now more easily be targeted by terrorists and extremists in online chat rooms, gaming platforms and other open and dark spaces online. Yet again, terrorists and extremists have introduced innovations faster than we have been able to respond, and as a result, have grown their digital advantage.

In this Spotlight, RAN practitioners, including the Working Group leaders of the RAN Communications and Narratives Working Group, share their insights on, and their work in addressing some of the different digital challenges, including transnational VRWE networks online, terrorists’ use of online gaming platforms, the organisation of mass protests via social media fuelled by conspiracy theories and radicalising narratives, and lone actors in digital environments.

Many of these topics have been addressed by RAN through Working Groups and small scale meetings during the first few months of 2021. The insights and experiences gathered from these meetings have been captured in a series of papers which will be published on the RAN website in the coming weeks.

As always, we want to hear from you! If you would like to contribute to future editions of Spotlight, or if you have ideas for an article, interview or feature, please get in touch with the RAN communications team at ran@radaradvies.nl

The RAN Staff
Contents

03  EDITORIAL  Digital transformation

08  ARTICLE  The Digital Gaps

12  ARTICLE  Transnational violent right wing extremism

20  ARTICLE  Online gaming platforms

26  PODCAST  RAN in Focus: Gaming

28  PROFILES  Meet the presenters

30  PAPER  Extremists’ Use of Video Gaming – Strategies and Narratives

32  FEATURE  The EU Internet Forum

36  ARTICLE  Young people online

40  FILM  RAN Reporters: Utrecht

42  FEATURE  Web constables

48  INTERVIEW  Facebook police

52  ARTICLE  Lone actors in digital environments

56  PAPER  Women’s Usage of Social Media and Lessons for PVE

58  LIBRARY  Discover More
ARTICLE: THE DIGITAL GAPS

Yet again during this COVID pandemic, terrorist and violent extremist organisations have proven adept at using the internet and digital technology to further their aims, reach new audiences and recruit people to commit violent acts. Government policies and responses at all levels have been in a state of constant catch up to ever changing technologies, adaptation and innovation by those who seek to exploit the internet for terrorism and extremism...

Dieter Loraine
We, as practitioners and policy makers, often try to address the terrorist and extremist influencing effort online through a limited number of traditional tools. Extremist organisations have institutionalised innovation as a means to reach, engage, impact and inspire their audiences. The wide-scale adoption of digital technologies due to the COVID pandemic has presented terrorist and extremist organisations, particularly violent right wing extremist (VRWE) groups, with new opportunities to radicalise and recruit. The gap between their use of digital technology to reach their audiences and our use of digital technology to do so and ability to respond has widened.

There have been five possible gaps in responding to the exploitation of the internet and digital technology. These are in: innovation, creative, knowledge, partnership and artificial intelligence. These gaps may not necessarily be new, but are increasingly becoming important to tackle.

1. The innovation gap – Terrorist organisations are fast to adopt and adapt to new platforms, often circumventing regulation and moderation to operate hidden in plain sight, leaving both internet service providers and policy makers playing catch up.

2. The creative gap – Terrorist and extremist organisations are experts at communicating with their audience, deploying the most relevant communication formats, channels and platforms with the latest and best production technology.

3. The knowledge gap – We live in a fast moving digital culture that is constantly evolving. Tracking shifting technology, culture and behaviours is impossible without clear communication and sharing of information, best practice and innovation between practitioners, private sector and government.

4. The partnership gap – There can be a disconnect between the private sector, communities, civil society organisations and government. Even with all the right intentions to collaborate there can be a lack of structure, shared language and frameworks that foster lasting partnerships.

5. The artificial intelligence gap - Terrorist organisations often outpace and outmanoeuvre the response by internet service providers and government in circumventing machine led detection.

By addressing these gaps effectively it is possible to reverse the trend and instead put governments and first-line practitioners ahead of terrorists and extremists and prevent their ability to exploit the internet and digital technology.

To do this, we must be quicker at adopting technology ourselves whilst using the reach and influence of digital technology to engage a creative and innovative response to the threat. Therefore we must strive to work more closely with the private sector and ensure a better flow of information between them, practitioners and government, in order to improve our understanding and application of new technology and AI and develop creative responses.

Dieter Loraine is Co-Founder of Albany Associates and a member of the International Digital Consulting Service, which helps governments harness the expertise and innovation found in the private sector.
ARTICLE: NEW THREAT? TRANSNATIONAL VIOLENT RIGHT WING EXTREMISM ON THE RISE

In the whole of the USA, 330 people have been killed by violent right-wing extremists in the past ten years. This is the conclusion of a report by the Anti-Defamation League (ADL). Meanwhile, in Germany, 182 people were killed in the past decade. According to the Global Terrorism Index 2020, right-wing extremist attacks have increased by 250 per cent worldwide between 2015 and 2019. During this period, there were 359 political terrorist incidents linked to violent right wing extremism, resulting in 190 deaths...
These numbers are stark and demonstrate the increasing threat posed by violent right-wing extremists (VRWE) who are increasingly networking transnationally. The virtual world is playing a decisive role in this. However, the phenomenon of transnational networking and cooperation is not a new one. There has always been networking and cooperation, through events, meetings, marches, at music festivals or at parties. The use of so-called mailbox systems in the early nineties, for example the “Thule network”, gave new possibilities for transnational networking and mobilisation. Since then, with innovations in digital technology the possibilities have been increasingly expanded and adapted.

With the increased use of the internet, right-wing extremist movements have been able to maintain day-to-day communication and cooperation. They use existing communication structures, through online gaming platforms or social media to do this, but have also developed alternative means such as alt-tech platforms, a group of websites and established their own online networks. By doing this, they create cooperative communication spaces that produce and reinforce extremist narratives.

**Franchise extremism**

With the emergence of the Identitarian Movement (Identitäre Bewegung), a kind of franchise extremism was established in Europe. Starting in France, branches of the Identitarian Movement were established in other European countries in varying quality and implementation. Nearly nine years after its foundation, the group “Generation Identitaire” was banned in France in March 2021. The ideological references of this Identitarian Movement are modified variants of cultural racist ideas that have their origin in the “Nouvelle Droite”.

In the process, the ideological narratives were delivered online to target audiences through campaigns or actions with media impact.
The special feature of this type of franchise extremism is its connectivity and thus its transferability to other European countries, since this form superficially rejects clear racist exaggerations and generates itself as a European community. The in-group and out-group are always defined in distinction to existing social values and systems.

After establishing itself in France, a branch of this movement developed very quickly in Austria, which became influential for other European countries. The Identitarian Movement thus developed a transferable model of transnational extremism, which uses campaigns and modern technology to turn cultural racist identity politics into a connectable franchise product for the first time.

An amorphous extremism via virtual structures

The terrorist attacks of the past decade in Utoya, Christchurch, Halle or El Paso, to name but a few, describe another face of this transnational connection. The perpetrators of the attacks mentioned did not know each other and did not belong to a common group. Nevertheless, they referred to each other, quoted each other in the execution of their attacks or staged their crimes as duplicates, or ‘copycats’, of previous attacks. What they have in common, apart from the implementation of their attack, is that they shared the same or similar narratives and used or consumed the same media.

In many cases, the possibilities that the internet offers for communication and individual reinforcement play a decisive role. Amorphous virtual groups such as the Atomwaffen Division (AWD) or the Feuerkrieg Division (FKD) operate almost exclusively in the virtual space with their networks and communication structures. The group was linked to deadly plots in Nevada and to a US soldier who allegedly planned to bomb CNN’s headquarters. Some of the members of these groups only know each other through this virtual space. Apart from a few meetings, the radicalisation processes take place on online servers set up for this purpose.

The groups recruit very young people, under the age of 14, as well as experienced and battle-hardened neo-Nazis from various parts of Europe and the United States. In the case of the FKD, sub-groups were formed in other countries, in addition to Estonia, Germany, England and the United States. These sub-groups planned or communicated their acts in the FKD network and then partly put them into practice. In many cases, there was no need for a larger control or chain of command. The members of these groups acted according to the principle of leaderless resistance and according to the narratives that were communicated within the group.

The link between digital and offline activity

In addition to these developments in the virtual space, cooperation in the non-digital world is also becoming increasingly more common. Right-wing extremist brotherhoods such as Blood & Honour or the Hammerskins already created these networks in the early nineties. The focus of networking was music and event culture, as well as marches and political events. These networks and structures are still active and are partly stabilised through parties from the extreme right-wing spectrum. Martial arts is another area that has not only become increasingly relevant in recent years, it is also the area that has become financially lucrative and attractive as a possibility for in-scene entertainment.

The events in Europe are not only for sporting competition. They are platforms for networking, a marketplace for the sale of merchandise, sports nutrition and propaganda, as well as a catalyst for conspiratorial cooperation and the testing of defensibility. The networks extend from Germany to Russia, Poland, Italy, Ukraine and Sweden. Events held by the scene have an impact that goes far beyond the regional level.

The development of transnational networks is not a new phenomenon or development. In part, it is based on developed structures. In doing so, the protagonists use the technical possibilities available to them and create narratives that can be connected across national borders and are catalysts.
“With the increased use of the internet, right-wing extremist movements have been able to maintain day-to-day communication and cooperation. They use existing communication structures, through online gaming platforms or social media to do this, but have also developed alternative means such as alt-tech platforms, a group of websites and established their own online networks.”

for mobilisation and action. Even if these developments are not new, they have reached a new quality. The individual possibilities of networking and communication, of self-staging and reinforcement from the respective reference group, have received an unprecedented boost through technical developments. Virtual reality can thus no longer be separated from offline reality; it is the impetus for action in the non-digital world. This is shown by these developments and not least by the countless victims of right-wing extremist terror.

Fabian Wichmann is a Working Group leader of the RAN Working Group on Communications and Narratives.
Video games have been stigmatised for many years, linked to many social ills including loneliness and terrorism. Not only is this often based on misguided prejudices and a misunderstanding of the gaming community in 2021, but this view risks robbing practitioners of one of the most exciting emerging methodologies in violence prevention: eSports to counter extremism...
Gaming culture often has systemic problems with race and gender. It is vital that these are tackled, however these imperfections do not define the gaming community. The view of gamers as socially isolated young men sitting in their parents’ basement is out of date. There are more than 2.5 billion gamers globally, almost 50% of gamers are women and the average European gamer is over 30.

Organised attempts to scapegoat some games for mass violence began over two decades ago in the aftermath of the Columbine massacre – the killers played games such as Doom. The NRA and other pro-gun groups attempted to direct public anger towards games and rock music to distract from the issue of gun control. This tactic of whipping up moral panic about the gaming community has continued ever since. Despite some well-funded attempts to problematise gaming, the American Psychological Association has stated that ‘attributing violence to video gaming is not scientifically sound and draws attention away from other factors, such as a history of violence, which we know from the research is a major predictor of future violence.’

As gaming and eSports (competitive gaming with spectators) have matured, a multitude of platforms have emerged to facilitate discussion, the sale and streaming of games. These platforms, the most well-known of which include Discord, Twitch and Steam, have now developed to a point where they can better be thought of as standalone social networks and e-commerce platforms. With the exponential increase in regular gamers and the corresponding rise in the number and complexity of platforms, it is unsurprising that these platforms have been abused by extremists. The perpetrator of the 2011 Utøya massacre was a gamer, the terrorist who carried out the Halle attacks streamed his crimes on Twitch, and there have been many high-profile references to gaming culture by far-right and Salafi-Jihadi extremists.

A recent meeting of the RAN Communication and Narratives Working Group found that there are six unique ways in which gaming has intersected with extremism: The production of bespoke games, modifying existing games, in-game chat, gaming adjacent
social networks, gaming cultural references and gamification. Each of these is distinctive, but many were found to have occurred rarely and had relatively little long term impact on extremist recruitment patterns, despite press attention. With significant proportions of the population enjoying eSports on a regular basis, it would be unusual if large proportions of terrorists and extremists were not gamers.

As ever, when studying extremism, mistaking correlation for causation is dangerous and counterproductive. In 2019, the RAN Youth, Families and Communities Working Group found that offline sports ‘can contribute substantially to the prevention of radicalisation.’ The same is true of eSports.

Like offline sports, video games offer participants the opportunity to find unity in a common passion, and to transcend physical, cultural, and linguistic barriers. eSports require high degrees of teamwork and communication; players need one another to accomplish missions or finish tasks. A 2019 survey found that 90% of gamers had experienced ‘some form of positive social interaction while playing online multiplayer games including making friends or helping other players.’ In times of severe isolation, as experienced during the COVID-19 crisis, having an online community can reduce loneliness. A 2020 report on video gaming in lockdown found that 30% of players say gaming helped them to feel happier and less anxious.

Practitioners hoping to use eSports as a tool to counter violent extremism need to go beyond tolerating video games and embrace the potential of this wildly popular medium. How to do this? Imagine eSports as offline sports and design programs to match. Arrange tournaments as diversionary activities, entice at-risk individuals to join specially trained eSports teams, and arrange intercommunity leagues. Embracing eSports will not only encourage practitioners to add much needed depth to their existing work, but will allow them to reach at risk users who never would have engaged with traditional offline sporting initiatives.

It is time for frontline practitioners to pick up a controller.

Ross Frenett is founder and CEO of Moonshot CVE and is a Working Group leader of the RAN Working Group on Communications and Narratives.

Joost S works as an analyst at Moonshot CVE and is a participating member of the RAN Working Group on Communications and Narratives.

“As ever, when studying extremism, mistaking correlation for causation is dangerous and counterproductive. In 2019, the RAN Youth, Families and Communities Working Group found that offline sports ‘can contribute substantially to the prevention of radicalisation.’ The same is true of eSports.”
RAN Practitioners has published the first in a new series of RAN Practitioners podcasts, called ‘RAN in Focus’. The podcasts, which are presented by practitioners from the RAN Practitioners network and hear from RAN Working Group leaders and experts in the field, will shed light on the challenges that RAN practitioners face to trending topics and the solutions they have developed in their intervention work. The first episode explores the challenge of terrorist and extremist’s use of online gaming platforms to radicalise and recruit.

You can watch the podcast in full on YouTube here.
PROFILES: MEET THE PRESENTERS

Jordy NIJENHUIS

Hi, my name is Jordy Nijenhuis. I am a storyteller, campaigner, consultant and trainer. I co-founded Dare to be Grey, an organisation that aims to counter polarisation. I am involved in a variety of campaigns and I train media professionals from all over the world in campaigning and countering radicalisation and disinformation. I believe that media is a powerful tool for behavioural change, and that we need new creative approaches to achieve fundamental change. I am delighted to be involved in the ‘RAN in Focus’ podcasts so that I can help to further explore the world of P/CVE and highlight all the important work that is being done within the RAN network.

Veera TUOMALA

Hello, my name is Veera Tuomala. I am a Helsinki-based Project Developer at Save the Children Finland. My primary focus is on RadicalWeb, a project that aims to prevent radicalisation and violent extremism in young people by training youth workers on early detection and dialogue. RadicalWeb is part of the current National Action Plan for the Prevention of Violent Radicalisation and Extremism. I have a keen interest in all things P/CVE and I am curious to find out more about the work being done within the network through the ‘RAN in Focus’ podcast.
Extremists’ Use of Video Gaming – Strategies and Narratives

Introduction

Although the use and abuse of not only video games but also gaming adjacent communications platforms and gaming imagery by violent extremists receives high-profile press attention, the nature and extent of this problem remains poorly understood by many frontline practitioners. The aim of the RAN Communication and Narratives Working Group (C&N) meeting held on 15 and 17 September 2020 was to explore this topic with practitioners, industry and experts. During the meeting, currently used strategies and narratives from violent Islamist extremist and right-wing extremist groups were presented and discussed. It became clear that a large variety of extremist propaganda and recruitment strategies can be identified, depending on the medium used (i.e. through games themselves, through gaming cultural references or through gamification). Used narratives include memes, symbols or other linguistic references to online gaming culture, the spreading of conspiracy narratives and the use of gaming jargon on platforms like 8chan. Additionally, challenges faced by first-line practitioners and policymakers were determined, after which some potential solutions to these challenges were identified. Rather than applying singular approaches (such as merely working on media literacy), it was suggested to apply multipronged approaches to tackle the issue from various angles at once. Attention was also given to ways in which the gaming community could be empowered to deal with the challenges, such as better access to reporting and notifying extremist content. This paper summarises the general challenges and the strategies and narratives used and recommends some practical next steps.
The EU Internet Forum:

Addressing upcoming VRWE challenges linked to new technologies.

The attack last January on the U.S. Capitol provides a perfect example of how the online dimension of violent extremism can easily lead to the perpetration of violence offline. In this case, the spread of conspiracy theories, which were amplified across platforms for weeks, contributed to the recruitment of extremists willing to carry out the assault, which brought about the death of four people.
The latest EU Internet Forum (EUIF) Ministerial meeting held on 25 January opened with a reminder of how the propagation and amplification of terrorist or extremist propaganda and conspiracy theories represents a serious threat to citizens’ security, since it might lead to violent actions and even murder. At the same time, the attack at the Capitol confirms another major concern: the need for better moderation of violent right-wing terrorist and extremist content.

A session of the meeting was dedicated to emerging challenges, with a special focus on new technologies used to amplify the propagation of terrorist, extremist and criminal content, such as algorithmic amplification, the misuse of videogame communication features, and other automated tools and strategies. A paper released by the EU Counter Terrorism Coordinator on algorithmic amplification presented at the EUIF Ministerial meeting highlighted risks related to the use of recommender algorithms to disseminate violent extremist and terrorist content online. While internet companies may claim that the risk is very low, law enforcement agencies and policy makers are concerned about a possible escalation in the use of new technologies by malicious actors to further disseminate their dangerous propaganda, radicalise and recruit.

The EUIF will further explore such phenomena, in order to support the development of effective prevention and response actions, in close cooperation with the internet industry and international partners.

The outcomes of these actions will be beneficial to the work of practitioners, as they will facilitate their understanding of the risks posed by new technologies and possible preventive approaches. Awareness raising on new technologies could enrich RAN activities on online-related issues, such as lone actors on the digital space, the phenomenon of violent Incels and their online environment (with possible connections to VRWE).

Finally, yet importantly, another emerging challenge that will be explored by the EUIF is related to the potential misuse of videogames to initiate users to violent extremist and terrorist content, with the risk of luring them towards extremist fora, platforms, websites or blogs via communication tools embedded in videogames. Gaming, especially as a consequence of the current pandemic, can offer the opportunity for violent extremists and terrorists to unite the emotional impact of videogames with political ideology. Young gamers may potentially represent a vulnerable target for these groups, for example when it comes to violent forms of gaming. The gamification of actions stemming from extremists’ narratives may result in a few individuals encouraged to score points by acting out violent actions offline.

Europol’s IRU is providing Member States with analysis on content identified on video games but the phenomenon needs to be further explored. RAN is also addressing this important issue in upcoming activities, including looking into what practitioners can do better to prevent the recruitment and grooming of vulnerable individuals through online gaming.

Read more about the EU Internet Forum [here](#).
Young people in Denmark are some of the world’s most insatiable users of online gaming platforms and social media. The English media researcher, Sonja Livingstone, has given them the nickname “more of everything”. They are at the forefront of digital use compared to many of the world’s young people. They are the first to get onto social media, the first to download apps, the first to do creative things – but also as a result potentially more vulnerable to digital bullying and radicalisation online. During the Covid pandemic it has become even more pronounced...
Today, in 2021, after a year of Covid, (social)-life is almost completely digital. Young people’s daily meetings and gatherings with other young people take place almost exclusively via digital learning activities, on gaming platforms and social media. They meet virtually with their (class)-mates on Zoom or Teams and socialise on Instagram, TikTok, Minecraft, Among Us or maybe in Fortnite – in combination with Discord and Twitch.

Before COVID, when young people came across fake news, or were in an online gaming situation where hateful rhetoric was explicit, they could talk about it at school with their friends and teachers. Their inner compass was adjusted each day. That is not a possibility during the COVID lockdown.

Young people are now spending much more time on their own. The potential echo chamber for radical views in many online (gaming) communities grows every day. Furthermore – many young people feel alone in the lockdown. And the common dynamics of these online communities is that members feel a sense of belonging. Over the last year there has been an increase from violent extremist groups trying to manipulate different gaming communities, often via Discord and Twitch.

In February 2021 the Municipality of Copenhagen launched a survey where 42 per cent of parents answered that they knew that their child had encountered statements that were hateful and derogatory about gender, sexuality, ethnicity, skin colour, religion, or social status of others, on social media and gaming platforms. 36 per cent had encountered conspiracy theories and misinformation, and 17 per cent had encountered calls for violence or other illegal acts on the basis of dissatisfaction with something in society.

What to do?
Unfortunately, there is no quick fix. In the 15 years I have worked on different issues regarding young people online, I have spent a great deal of time educating or developing information materials for young people, parents and teachers alike. When it comes to the digital world, adults have a very different understanding and awareness to young people. So, it takes effort and a variety of different approaches to communicate or even translate the digital world of a young person to adults. Often, it is beneficial to look beyond the digital and talk about the emotions that can be spurred by encountering hate speech and violent pictures or videos.

At Save the Children Denmark we have done that in a lot of ways, eg. web materials, podcasts, articles, campaigns, and the education of professionals working with young people. Recently we released the app SoMeDigMig (SoMeSoYou) which holds more than 400 questions that can be used to start a conversation between young people and adults about the digital world – especially gaming. We could see that the intention to talk to young people was there. Adults just did not know how to ask questions to children about the digital world without being condescending.

About seven years ago, I had taken a youth panel to Istanbul to speak at the IGF, an international conference about young people online. During one of the sessions about picture sharing and the right to be forgotten – one of the adult experts proclaimed to the young people talking, “You have too many crazy ideas!” Nevertheless – one of the crazy ideas was a service that could help young people delete pictures online. And like that – the idea behind one of the game changers for digital child wellbeing was born. The “Delete It Helpline” – where young people in Denmark have been getting help deleting videos and pictures online since 2016.

I often think of that moment... on how the young people became the role models for us all, with their entrepreneurship and imagination. They are the experts on their own lives. And we better listen to them. So maybe that could be a good place to start. Enter the gaming world with a young person. Watch them play ... and just listen!

Jon Kristian Lange is a senior advisor at Save the Children Denmark.
RAN Practitioners has published the first episode in a new series of programmes, called ‘RAN Reporters’. The new programme sets out to uncover some of the most interesting and timely stories from the RAN network, showcasing the work of individual projects, initiatives, interventions and campaigns delivered by RAN practitioners. The first episode travels to Utrecht in the Netherlands to hear how practitioners from different working fields came together to prevent a riot in the wake of new COVID lockdown measures introduced by the government.

You can watch the programme in full [here](#).
Artificial intelligence robots are smart and can be used and support us in various ways on the web. However, there are currently no robots which can sufficiently help victims or potential victims of crimes who want to speak to someone or report people online.
These can be people who are afraid of the person they’re living with, children who feel uncomfortable with their trainer-instructor, or those who are bullied on social media because of their beliefs. In Estonia, it is possible to write a Facebook message or send an e-mail to a specific police officer, who we call ‘web constables’. The main goal of these web constables is to be active on social media and be there for people.

The idea of web constables is not new and was based on an approach that the Finnish police has been doing for the last ten years. In Estonia, we have three police officers working as public figures on Facebook: two Estonian-speaking officers and one Russian-speaking officer – Russian is spoken quite widely throughout Estonia. We have two male and one female officers. In my experience, gender only matters when people have questions about the Traffic Law: male police officers get them almost three times more.

The idea to be visible and reachable on the internet as a police officer is especially important right now, given people are spending large amounts of time at home due to the COVID pandemic. People are stressed, bored, anxious, lonely and are spending more time on the internet. This is good news for criminals. Some of the problems that we have seen lately include:

— The rise of fake news. If people do not have a place to turn to and ask questions, they can start to believe in false information, such as that around the COVID pandemic and vaccination programmes.

— The rise of scams. People who would usually spend their money on holidays, shopping or entertainment are now thinking about investing their money instead and are therefore becoming susceptible to online scams.

— The rise of grooming on the internet. With young people at home and taking lessons online they have more access to the internet than ever before. An example is that more young people are playing online games where they can communicate with strangers.

— Radicalisation. Governments are instructing people to stay at home, wear masks and have vaccinations. Meanwhile, most shops and public spaces are closed. This combined is having a dramatic impact on people’s daily lives. The internet is full of people who are angry and spread hate speech. Some of these people also call for others to commit illegal actions. In many cases it is possible to contact them via Facebook, remind them of the law and avoid those actions.

Web constables are in a position where they can support people, explain the law, give guidance (how to recognise fake profiles, fake news, scams), where to turn in case of victim support or mental health etc. We don’t care if the need for help comes under a real or fake name, because the idea is to be there for everyone. If something needs police investigation then they are there to guide people.

I am well aware that our system of three web constables for a whole country works only in Estonia. Our country is small. Our communities are small. We intend in time that every local constable will have their own social media account and can be part of their own small communities online. It just takes some time.

My tip for other countries? Try to be as close to people as possible. Mistakes on social media are okay, apologise if needed. Be honest, but don’t replace human contact with report sheets and AI. For the last five years, approximately 90% of people in public opinion polls say that they trust Estonian Police and Border Guard Board. We must have done something right and I believe that being present on the internet, where people need us the most is one of the key reasons. (But for trust to develop that much, you have to do all your police tasks to the highest level!)

Maarja Punak is communications officer and former web constable in the Estonian Police and Border Guard Board.

Find more examples of projects on digital police work in the RAN Collection of Inspiring Practices here.
How did it all start?

In 2011 my police station started its first official Facebook page, a new trend that was just beginning with the Swedish police. At the time I was the officer in charge of the youth squad so they thought it would be best if my group was involved. But I was not interested. Not because I thought the police on social media was a bad idea. I was just not interested in social media.

Unlike my colleagues, family and friends I did not have a private Facebook account, Instagram and LinkedIn were unknown to me and the closest I had ever been to a tweet was in the bird section of the local pet store. It just wasn’t my thing.

After a period of back and forth with the police communications department where the words “please” and “no” were exchanged countless times, they finally convinced me to say “yes”. It became a little side project where my normal police duties would take priority and Facebook updates would be written when, and if time allowed.

How successful were you in the early days?

I was destined to fail from the beginning. I had never had media or communications training, had no experience on social media and to top it off I was going to be posting updates in Swedish, which is my second language. I moved to Sweden from Australia 11 years prior and although I had learnt the language well enough to be a police officer I soon learned that even a poorly placed comma would wake the screaming masses of offended “language experts” online.

We started with very simple updates. Photos and posts of traffic duties, information about when our local police stations were open, warnings about crime trends. It was a paradigm change within the police. An organisation that was traditionally restrictive with information was suddenly opening up.

“Build it and they will come” is not an accurate phrase you could use for our Facebook page. No one was following us. One day after a long shift, I checked the traffic duties update that I had...
posted a few hours earlier. I was excited to see that 18 people gave the post a thumbs up. When I checked to see whom these people were I discovered that it was none other than the chief of the traffic police and 17 other colleagues. In other words, we were not reaching the people that mattered – the public.

**How did it become successful?**
I had lost interest very quickly and stopped updating. My colleagues continued but I went silent. After about a month the communications department wanted to know why I had stopped. It was at this point I decided to change tact. I made a conscious decision to not only write about our duties but also to give advice and points of view in a way the public is not used to hearing from the police. My updates always had a message from the police, it was often woven into a humorous tale and not always obvious, but it was always there.

Along the way, I learned a few very important things: 1. Humour and irony work, but it is a balancing act; 2. Messages, points of view and advice are much easier to convey if they are woven into a story; 3. Never aim messages, points of view and advice directly at the target group. Cognitive dissonance is a poisonous fruit of ideology. People with cognitive dissonance will never accept another point of view if they think they are going into battle. I assumed that these people could read my posts and if I could get a message across without going into direct combat there was the possibility of planting a seed of sense or doubt.

The "little side project" that we started became much bigger than we ever expected. The aim was to get information from the police out to the local population. Instead, the messages from our small local police station were reaching all over Sweden and beyond. Many individual posts had millions of views. The police in our neighbouring countries of Denmark and Norway were translating some of our posts and reposting them on their own Facebook pages. One of our posts was even translated into English and written about in the Washington Post.

**Any final comment for practitioners?**
My career has taken me in another direction now and I no longer work as a “Facebook police officer”. But after 24 years as an operational police officer, I can say that social media, if used in the right way, is the most effective messaging tool the police has ever had.”
The Halle attacker – who killed two people, injured two and aimed at killing dozens more at a Synagogue on 9 October 2019 – was inspired and motivated by online manifestos. In addition, he streamed his attack online and posted his own manifesto online, too. His attack has been marked as a typical ‘lone actor’ attack...
‘Lone wolves’, ‘lone actors’, ‘solo terrorists’, ‘loners’, ‘lone attackers’ – all definitions suggest a single individual, finding his or her way into an extremist ideology without affiliating to a group or network and operating on their own. However, most of the so-called ‘lone actors’ who carry out attacks subscribed to certain narratives and unorganised collectives. These collectives are leaderless and without clear hierarchies, but their followers are connected and united by shared narratives, values and enemies. For example, during his trial, the Halle shooter said that he did not join any group since he thought they would all be under surveillance. But he made clear that he feels like a soldier fighting for the “white race”.

RAN Practitioners has organised a number of meetings to discuss the topic of “lone actors”, and one outcome of a recent meeting is very clear: so-called lone actors usually are neither alone nor do they feel lonely. This makes the narrative of ‘lone actors’ inaccurate and potential harmful. It might lead to the underestimation of the milieus and informal networks that provide ideological, moral and sometimes logistical support to lone attackers. Online and social media platforms clearly provide the means for “lone actors” to be recruited or to self-recruit, to meet others and to consume terrorist narratives. Having said this, terrorism in most of its forms has existed long before social media.

Social media companies have invested resources into content moderation tools and procedures to diminish violent, hateful and extremist speech online. They also partner with specialist organisations in the field of P/CVE such as MoonshotCVE. A concrete example of this was the one-to-one online intervention approach designed to fill the gap of not having systematised attempts to supplement counter-speech efforts with direct online messaging and engagement at scale. Delivered on Facebook to date and working across VRWE and violent Islamist ideologies, the programme provides an opportunity for individuals showing clear signs of radicalisation to meet and engage with someone that can support their exit from hate. Furthermore, MoonshotCVE helps them to identify hotspots, narratives and terminology related to radicalisation online.

However, significant challenges remain and more resources should be invested by the companies to make their services safer for users. While the immense amount of user-data might make it difficult to look for terrorist content, the platforms are able to scan, process and monetise all user data. First-line practitioners face the challenge that they are often told to ‘be present online’, but do not necessarily know exactly which platforms or websites are relevant, how to behave and communicate online and what risk indicators to look out for. Especially within certain groups, such as the recent phenomenon of Violent Incels, so-called shitposting and violent language is a key element of their way of communication. Differentiating between noise and relevant signals, and low-risk and high-risk individuals, is therefore hard.

Secondly, the digital landscape in which lone actors operate changes constantly. For social media companies and online platforms, it is a constant ‘cat and mouse’ game: a game of constant pursuit, near captures and many comebacks. If extremists are removed from certain platforms such as Facebook, they move to others, such as 8Chan or Telegram.

The recommendations for preventing and countering “lone actors” from turning to violence largely resemble P/CVE strategies that were already in place within RAN over many years. It is key to maintain existing efforts to properly understand individuals and their pathway to radicalisation. We need to learn from debriefings, trials and research. Practitioners need to be trained to understand trends, narratives, memes, insignia of online extremists milieus and need to be able to engage in conversations with individuals vulnerable to radicalisation. This makes them able to detect specific warning signs.

On the side of policy, the dialogue around and pressure on social media and online-gaming regarding their efforts to not only de-platform terrorist content but to identify potential digital “lone actor” terrorists in a proactive way, need to be kept up. Lastly, it is key to invest in policy-oriented research on this phenomenon, and more particularly, into identifying digital milieus where potential “lone actors” are active, so we don’t misunderstand and then miscalculate the threat terrorists without formal ties to organisations pose.

Alexander Ritzmann is a Senior Advisor to RAN and the Counter Extremism Project.
10/12/2020
CONCLUSION PAPER
RAN Small Scale Meeting
24 November 2020, Digital Meeting

(Young) Women’s Usage of Social Media and Lessons for Preventing Violent Extremism

Key outcomes

The perspective on the role of (young) women in extremism has changed over the last years towards better understanding of how women radicalise, how they are recruited, and what their role in terrorist or extremist organisations can be. For many years, the public view on the agency of women has been neglected or marginalised. With substantial numbers of women travelling to Iraq and Syria to join Daesh, this view has changed. Despite the relatively large amount of research done on gender and radicalisation/extremism, there are still considerable gaps to fill. While the focus of the recent years has been on Islamist extremism, women and other forms of extremism have been rather understudied.

One of the main challenges for an effective intervention is the fact that much of the interaction has moved online. Studies have shown that women spend more time on social media than men and that the internet and social media can serve as a gateway to extremism. Therefore, the (online) radicalisation of women in different extremist settings needs to be explored further and understood to a degree that practitioners can adjust their intervention accordingly.

The RAN small-scale expert meeting on (young) women’s usage of social media and lessons learned for preventing violent extremism (PVE) was aimed at unpacking some of the gaps. This paper summarises the highlights of the discussion, discusses the vulnerabilities that are specific to (young) women, explains how recruiters use these vulnerabilities online and, finally, presents the recommendations that the experts stressed during the meeting.

A RAN Practitioners paper, published in 2020, provides insights for practitioners on how women radicalise and how they are recruited online in different extremist settings. The paper details the vulnerabilities of young women and provides a series of recommendations for practitioners on how to adjust their intervention accordingly. You can read the paper in full here.
IF you would like to discover more about the topic of youth engagement you can get in touch with the RAN Staff, take a look at the RAN Collection of Inspiring Practices or read through some of the latest RAN papers. We have included some of these papers in a carefully selected collection of interesting and relevant articles below.

RAN (2020)  
‘Extremists’ Use of Video Gaming – Strategies and Narratives’

RAN (2020)  
‘Galvanising youth in combating online disinformation’

RAN (2020)  
‘P/CVE and mental health support online’

RAN (2020)  
‘Harmful conspiracy myths and effective P/CVE countermeasures’

RAN (2020)  
‘How to do digital youth work in a P/CVE context’

RAN (2020)  
‘Women’s Usage of Social Media and Lessons for PVE’

RAN (2018)  
‘The role of police online in PVE and CVE’
This publication has been commissioned by the European Commission and has been prepared by REOC Communications on behalf of RadarEurope, a subsidiary of RadarGroup.