SPOTLIGHT
SEPT 2021

EMERGING THREATS
As vaccination programmes continue to be rolled out across Europe, and government restrictions in some places relaxed, we can begin to contemplate life after COVID. However, the work to address some of the long-lasting consequences of the pandemic on individuals and communities has only just begun.

In the last year we have seen the emergence of a new set of P/CVE threats. Not only has the pandemic accelerated a number of nascent threats emerging in early 2020 but it has also given terrorists and extremists new opportunities to radicalise and recruit. Our job as P/CVE practitioners is to recognise these emerging threats, understand them, and develop and deliver effective interventions and responses to tackle them.

In this Spotlight, RAN Practitioners and Working Group leads share their views, insights and their work in addressing some of these threats, including emerging violent right-wing extremism (VRWE) accelerationism narratives, a look into the new and quietly developing violent Incel movement, as well as lone actors in an increasingly transformed digital world.

Many of these topics have been addressed by RAN Practitioners through Working Group 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 Practitioners 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 Practitioners communications team at ran@radaradvies.nl

The RAN Practitioners Staf
This year marks the 20th anniversary of the events of 9/11, the catastrophic terrorist attack that took the lives of 2,977 people and injured 6,000 more. In total, citizens from 90 different countries were murdered by al-Qaeda that day. Just over a decade later, Daesh reared its head and recruited as many as 30,000 thousand followers from 85 countries.
While we, our governments and their security apparatus were transfixed by the gruesome Islamist endeavours playing out in Syria, Iraq, Afghanistan, Mali, Nigeria and Somalia, and the risks they might pose to our own communities, a new threat was gestating in the corners of the internet. Right-wing terrorism was finding a new lease of life with isolated and forgotten individuals in cyberspace, while far-right protest movements mainstreamed extremist ideas.

Programmes to prevent or counter violent extremism – P/CVE - have evolved across Europe and balanced the brutality of the terrorists with a positive, social care approach to stop the descent into violence of an increasingly disenfranchised youth. By understanding the ‘push and pull’ factors that enable radicalisation, practitioners can help people find a pathway that reduces the relevance of extremist movements and provides a sense of purpose and belonging. Positive activism replacing violent agitation.

The work has never been easy, and many will tell you they feel they are struggling to make the wider societal difference they would like, instead only being able to focus on individuals. However, it is important to remember that for that one person, it is providing a lifeline to a better future. All practitioners should be confident of the impact they are making in difficult circumstances.

Twenty years after al-Qaeda forced its way into the public eye, the fear is that things may be able to get worse. The global Covid-19 pandemic has been a gift to terrorist recruiters. Conspiracies, disinformation and a lack of trust in governments are the lifeblood of extremist narratives and the pandemic has delivered these on steroids. Seemingly sensible people firmly believe that 5G technology is transmitting the virus or that vaccines contain microchips to bring us under the control of Microsoft.

Lockdowns, restrictions on our freedoms and chaotic decision-making have fractured an already fragile trust in government and disinformation has spread across social media, amplified by malicious states to create mayhem. To compound these issues the very nature of radicalisation and terrorism is evolving faster than we can react.

Traditional, coherent ideologies are fracturing as cohesive terrorist groups lose their relevance and vulnerable individuals - those more susceptible to extremist narratives - select piecemeal fragments of different ideologies to satisfy intensely personal grievances. This ‘pick n mix’ radicalisation - driven predominantly by the online amplification of ideologies and grievances - not only places greater emphasis on underlying social fractures and psychological factors but has led to the age of those needing support for radicalisation plummeting, something identified in Europol’s most recent TE-SAT report.

Terrorism laws, so effective at targeting groups and terrorist cells, can appear impotent in the face of self-initiated terrorists (lone actors) whose signposting of their intentions is indistinguishable from a cacophony of ‘edgelord’ keyboard warriors and a younger cohort of individuals engaging in terrorism-related activities for whom social care or mental health support is a far better solution than enforcement or prison.

In fact, the kaleidoscope of underlying psycho-social factors that increase susceptibility to radicalisation, while well-known, do not always fit easily with counter terrorism policy, where the money for such initiatives normally resides, nor should they necessarily be delivered through a counter terrorism lens. This inconsistency over who should be responsible hampers progress and creates anxiety in communities. Lastly, there can be a timidity in publicly rejecting the ideology of Islamist extremism for fear of offending Muslims. However, Islam is a religion, whereas Islamism is a political project. To conflate the two is the real insult to Muslims.
But there is a silver lining. The foundations built by P/CVE have never been more relevant. Spotting behavioural changes in societies most susceptible is now more critical than ever before and friends, families and frontline workers are still best placed to identify those close to them who need support. Tech-savvy companies are developing tools for identifying radicalised individuals online and municipalities should now be adept at targeting their resources at highly localised hotspots of extremist activity.

This hyperlocal approach is going to be critical for the long-term disruption of radicalisation networks. Instead of a costly and less effective broad-brush approach to P/CVE funding and delivery we must home in on the small geographic areas within a town where these issues coalesce and utilise every tool at our disposal: counter terrorism, counter radicalisation, counter polarisation and counter disinformation methods sitting alongside the promotion of shared values, a common identity and a network of NGOs and municipality practitioners to offer bespoke interventions for the most vulnerable.

If we can simultaneously deliver an acute, hyperlocal response and collectively be resolute in our total rejection of the ideologies themselves, we can not only weather the incoming storm, but I’m confident we can start to turn the tide.

WILL Baldet is a Policy & Practitioner Fellow at the Centre for the Analysis of the Radical Right (CARR) and is a Senior Advisor to the UK Government on Prevent.
Accelerationists (who want to instigate a race war to bring down liberal democracies), saw the COVID-19 pandemic, the different health related measures and restrictions, and the surrounding fear, confusion and criticism as an opportunity to benefit from the resulting societal polarisation. Fortunately, their apocalyptic narratives seem to have found little to no relevant support beyond already affected RWE milieus.
Nationally and transnationally, violent right-wing extremist (VRWE) actors feel connected through narratives such as the “Great Replacement”, the “White Genocide” and the “Day X”.¹ Those narratives claim that there is an existential threat against the white race due to the presence and influx of non-white foreigners which will supposedly lead to a new “brown” race. This, VRWEs say, needs to be avoided at all costs. Furthermore, feminists are seen as a major threat and therefore feminism is made responsible for shrinking birth rates. According to VRWE propaganda, all this is part of a worldwide Jewish conspiracy to exterminate the white race. This proclaimed apocalyptic dimension provides the justification for violence, framed as “self-defence”.

It is important to highlight that the “Great Replacement” and the “White Genocide” do explicitly not focus on nations but on the “white race”. Transnationally-oriented VRWEs say that the attack against the “white race” can only be countered if white “nationalists” cooperate. Or put differently: The “white race” can only be saved if all VRWEs work and fight together.

Not only do (or did) groups like the German “National Socialist Underground”, the Finish “Soldiers of Odin”, the Scandinavian “Nordic Resistance Movement ” or the US “Atomwaffen Division/ National Socialist Order” promote those narratives and conspiracy myths, but so-called ‘lone actors’, who carried out attacks in Pittsburgh (USA, Synagogue/Jews, 2018), Poway (USA, Synagogue/Jews, 2019), El Paso (USA, Supermarket/Migrants, 2019), Oslo (Norway, Mosque/Muslims, 2019), Halle (Germany, Synagogue/Jews/Migrants, 2019) and Kassel (Germany, Assassination of pro-immigration Politician Walter Lübcke 2020), refer to these narratives specifically.

Strategy wise, VRWE terrorists can be put in two camps. Firstly, the “root causes” camp aims at killing Jews and politicians, since they are supposedly responsible for the ‘problem’ itself, be it immigration, feminism or liberalism. Secondly, the “accelerationist” camp claims that democracies are already dying, but not fast enough. Their attacks aim at provoking a race war.
Accelerationists differ from other VRWEs in the way that they want to start a civil war between “whites” and non-whites, Muslims, Jews, feminists and their supporters on a “Day X”, which they claim should happen as soon as possible. Several attacks against Muslims in particular were explained by the perpetrators as targeted provocations with the aim to generate a violent reaction from Muslims.

Accelerationism was, for example, promoted in the “manifest” of Brandon Tarrant (New Zealand, Mosques/Muslims, 2019), who proclaimed Anders Breivik (Norway, Government employees / Political youth Camp, 2011) as his “hero”. Breivik himself referred to Timothy McVeigh (USA, Government employees/Kindergarten children, 1995). In their manifests, those terrorists refer to the right-wing extremist apocalyptic and accelerationist “Turner Diaries”, a novel (USA, 1978) describing a post-nuclear race war. Another key accelerationist publication is “Siege” (USA, 1992), which is also mentioned by many so called ‘lone actors’, which calls for independent terror cells to start a race war. Those decades-old narratives seem to have contributed to a new leaderless transnational apocalyptic VRWE movement that feels connected through shared narratives, values and enemies.

At the same time, some more traditional right-wing extremist groups that aim at overthrowing liberal democracies without starting a civil war actually distance themselves from accelerationist groups, actors and narratives. Examples include the “Atomwaffen Division” or the Halle and Christchurch attackers, because to them accelerationists are “too infantile, extreme, unserious, and essentially hurting their cause”.

Accelerationists also potentially conflict with the proposed future counter-society narrative of those traditional VRWE that promote a happy, pure and safe (whites only) community. This strategic split within the VRWE scene should be explored further as a means of tackling prevailing extremist narratives within P/CVE activity.

Alexander Ritzmann is a Senior Advisor to the Counter Extremism Project (CEP).
Contemporary manifestations of violent right-wing extremism in the EU: An overview of P/CVE practices

A RAN Practitioners paper, published in 2021, explores whether measures to deal with previous violent right-wing extremist threats are fit to counter current manifestations of violent right-wing extremism (VRWE). The paper describes the modern VRWE scene and how it has evolved, and highlights a number of promising practices from previous programmes targeting right-wing violence. The paper can be read in full here.

Contemporary manifestations of violent right-wing extremism in the EU

Position towards politics. Some right-wing extremist movements approach their battle as a long march through the institutions. Identitarian movements engage in a metapolitical battle: they participate in the political process and try to place members or followers in strategic positions in public institutions to influence the wider political debate in society (12). Also, some neo-Nazi groups have been involved in electoral politics. The Nordic Resistance Movement is a legitimate political party in Sweden, where it stood in the 2018 national elections. On the contrary, other accelerationist groups, such as the Siege Culture neo-Nazi groups, reject the political (and societal) system as a whole and aim to overthrow it through violent actions.

Trends in right-wing extremism

Internationalisation

Right-wing extremist individuals and groups have long been very well connected internationally. In previous decades, international contacts facilitated the spread of strategic and tactical concepts and inspired the creation of local chapters of organisations (13). Yet, recent technological advances have accelerated and deepened the internationalisation of the right-wing extremist scene. Web 2.0 tools fuel international connections and facilitate the exchange of strategies, tactics and know-how. International links exist in all different sub-currents of right-wing extremism: Neo-Nazi organisations, ultranationalist movements and Identitarian movements maintain extensive international links with other individuals and groups. This transnational VRWE movement is, for instance, connected through the participation in political marches and rallies (e.g. the Day of Honour in Budapest), violent sports (in particular Mixed Martial Arts, see also the RAN paper on sports and P/CVE), and music events (14). Also the current spiral of violence by lone-actor terrorists (15) is an example of the internationalisation of the right-wing extremist scene:

“...”

Today’s interactive internet also enables right-wing extremists to reach a global audience and has created new means to radicalise and recruit followers and sympathisers. For instance, some right-wing terrorists showcase their attacks to a global community by livestreaming them and spread their radical narratives through online manifestos (17).

The internationalisation of the right-wing scene also takes places in the offline world. Extremists participate in concerts and rallies abroad to forge stronger personal and organisational links with other likeminded individuals (18). The conflict in eastern Ukraine, in which thousands of foreign fighters participated, constitutes a hub in the physical network of the VRWE scene (19).

(11) Bjørgo, Right-Wing Extremism in Norway.
(12) Metapolitics is defined by Nouvelle Droite theorist Guillaume Faye as the “social diffusion of ideas and cultural values for the sake of provoking profound, long-term, political transformation”.
(13) See, for example, Koehler, The German ‘National Socialist Underground (NSU) and Anglo-American Networks.
(14) Counter Extremism Project, Violent Right-Wing Extremism and Terrorism, p. 6.
(15) Lone-actor terrorists are not as isolated as the terminology suggests. They frequently have interpersonal, political or operational ties to larger networks. They also often radicalise both in online and offline radical milieus and sometimes receive concrete assistance in the preparation for their attacks. See, for example, Bouhana et al., Background and preparatory behaviours of right-wing extremist lone actors.
(16) The Soufan Center, White Supremacy Extremism, p. 11.
Interview: Terrorist exploitation of online gaming platforms

What is the nature and scale of the radicalisation threat on online gaming platforms?
There have been occasions when violent extremists have attempted to hijack gaming cultural references by taking over certain popular games. As a society we shouldn’t play into their hands. Irresponsible journalists, practitioners and policymakers can unknowingly create a propaganda coup by reporting such attempts as a bigger threat than they actually are. There is very little evidence that these activities are being organised on a strategic level in terms of engagement with at-risk audiences.

When you see gaming being highlighted as an ‘emerging threat’ in the world of P/CVE, what is your reaction?
Gaming and the use of gaming platforms can be highlighted by journalists and practitioners in the aftermath of an attack when it emerges that perpetrators have engaged in gaming in the past. However, it is important that we realise that the vast majority of people in North America and Western Europe have played computer games in the past and there is not necessarily a causal link.

Do you think that gaming platforms therefore present just as many opportunities as they do ‘threats’?
Yes! I think gaming platforms present a huge opportunity for P/CVE practitioners. In the same way as it is very common to see P/CVE programming that utilises sports and other common hobbies as a way of engaging people, we should see gaming in the same way. For example, e-sports and competitive gaming can be integrated into violence prevention efforts. The sooner that happens, and gaming is no longer problematised, the better.

What tips would you give to practitioners, particularly those that may not be very attuned to gaming platforms?
Learn! The vast majority of young people in Europe and North America are gamers. As a practitioner that works on these issues it’s not an option to not have a grasp of the hobby that is so common amongst your target audience. An understanding either personally or on your staff of gaming and the culture that underpins it is vital to any practitioner that is working on...
violence prevention, especially when it is so important to many young people and their identity.

**How can gaming and gaming platforms be harnessed for good P/CVE work?**

Gaming can potentially be used in violence prevention in two different ways: Community outreach and connection is often key for areas experiencing inter-community tension. Practitioners bring kids from divided communities together to reduce tension by using sports such as football. Gaming and e-sports could be used in much the same way.

In the case of countering violent extremism, gaming can be used by intervention workers and others to build trust with individuals who are already engaged with extremist material, or are further down the radicalisation funnel.

**What do you see as the future for gaming in P/CVE?**

In five years I’d like to see an end to the stigma from policymakers and practitioners that surrounds gaming. Gaming, gaming adjacent communications platforms and gaming culture should, instead, be integrated into their violence prevention efforts.

“In the case of countering violent extremism, gaming can be used by intervention workers and others to build trust with individuals who are already engaged with extremist material, or are further down the radicalisation funnel.”
In our new series of podcasts, ‘RAN in Focus’, we have been exploring and dissecting some of the emerging P/CVE threats. The first podcast, released earlier this year, looked at how terrorists and extremists have been using online gaming platforms to radicalise and recruit. Check out this episode on the RAN YouTube channel now, soon to be available on Spotify. You watch or listen to the podcast in full here.
2011–2013 Acceleration in widespread use of social media platforms.

2013 Rise of so-called ISIS

2014 Flow of FTFs to Syria and Iraq

2015–2017 Surge in Islamist-inspired terror attacks

2016 Increase in spread of disinformation

2018 Fall of the so-called Caliphate

2018 Return of FTFs and their families

2018 Increase in left-wing extremism

2018 Return of FTFs and their families

2018 Increase in spread of disinformation

2018 Fall of the so-called Caliphate

2019–2021 Rise of VRWE violence

2020 Increase in left-wing extremism

2020 Emergence of Incel movement

2021

RAN Timeline
10 Years of Threats

September 2021
Emerging Threats

October 2021
Emerging Threats
Incels - people living in ‘Inceldom’ - define themselves by their inability to engage in romantic or sexual relations, despite strong wishes to do so. A true Incel is someone who has not, and never will, engage in any such activities or relationships. People referring to themselves as Incels are mostly portrayed as perpetrators of violent criminal acts or by shock-and-horror stories in tabloid newspapers.
Lurking in the deep and dark corners of the internet are the social misfits and sexually frustrated Incels. They spew misogynistic hate speech, promote rape and pay tribute to mass-murderers and terrorists. Analysis of the incel phenomenon range from those who believe them to extremely dangerous and should be stopped at any cost, to those who believe taking such a narrow view risks simplifying a complex social structure. Therefore over the years, I myself have observed, monitored, interviewed and tried to understand Incels – both as a collective, and through some individuals who agreed to give interviews. Therefore, this article represents my main observations and insights.

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...
The Evolution of the Incel Movement

The term ‘Incel’ (a portmanteau of involuntary celibate) was coined in 1993 by ‘Alana’, a young woman struggling to find love. Since then, through a series of digital transitions and reformations over online communities such as love-shy, 4chan and Reddit, the Incel community has found its voice, with occasional spillovers into social media.

The connotations of the term itself has changed drastically since its digital birth in the early 90s. It started as a moniker proclaiming feelings of loneliness and estrangement from “normal” peers. Originally, it focused on coping strategies, personal development and expressing the frustration of feeling ostracised from partaking in flirting, giving or receiving romantic attention or having sexual relationships. It has since grown to a community expressing frustration, anger, and antagonisation of non-Incels (“normies”).

Threads with titles such as: ‘Women should be kept uneducated’ and ‘Hitler, and a better world – my Neo-Nazi visions’ are just a few of the offensive and aggressive discussions on the front page of one of the most prolific Incel discussion boards (their communities have mostly been banned and outlawed on Reddit, Facebook, Twitter etc.). Keeping women uneducated or installing extreme political governments to enforce the fantasies of controlling society is a pivotal point in the societal focus of the Incel community. As such the Incel community places itself as part of the manospheric wing of the internet, which is a newer movement focusing on the inherent higher value of men in the world at large, whilst simultaneously continuously attacking feminism for its attempts to bridge the gender divide between men and women.

Therefore, Incels are currently a growing body of concern for many institutions, particularly as the threat continues to grow. Although Incels have headlined newspapers following horrible attacks in Isla Vista, Toronto, Tallahassee, Parkland amongst others, the growing number of threats and violent communications made online has caused police in both the US, Canada and Europe to pre-emptively apprehend an increasing number of young men threatening or even planning to commit comparable atrocities and attacks. This increase has led several national security services to include Incels in threat-status reports (Denmark, Sweden, US, Canada, England and many more).

Incels - Part of 'The Manosphere'

As part of the Incel anti-feminism that seeps from closed forums and into mainstream and social media, we also observe a disproportionate level of threat, hate-speech and digital attacks aimed at female politicians and media personalities, particularly against those with a clear feminist or progressive narrative. This leads to many activists silencing themselves out of fear for attacks. Indeed, the Institute for Human Rights (Denmark) and data-analysis organisation Analyse & Tal (Analysis & Numbers) have both proven that women are targeted far more frequently than men in these cases.

Although the framing of Incels can easily lead to painting a picture of violent criminals congregating in online environments to plot revenge and political violence, this is far from the case. When observed, it becomes evident that many new users join such communities to find a place to fit in; they express a self-narrative of loneliness, unpopularity, low self-esteem, and low social status, all of which makes it impossible for them to take part in youth culture. However, what could have been an online support-system quickly becomes toxic.

When interviewed about angry and violent sentiment put forth online, almost all Incels have given statements describing extreme ostracisation, loneliness, unhappiness and other extremely negative upbringings. This in no way excuses the violent rhetoric they author online, but combined with other knowledge about men's ability to emotionally express themselves, we need to understand the possibility of Incels “translating” emotions, experiences and their whole lives of sadness and unhappiness, as these are not generally accepted masculine emotions, into those of anger, violence and revenge.
The problem - and solution - to Inceldom

Observing Incel forums also brings further evidence to support this notion. Many users seem to begin their digital participation by asking support-seeking questions. To give one example, on a prominent Incel forum, one user first asks in 2018: ‘What’s wrong with me?’ Two years later, the user posts a new question: “How many foids could you kill in a fight?” (’Foid’ is an extremely derogatory term used in objectifying women). The first question was met with replies blaming women for his vulnerability.

This process has a profound effect: It necessitates the Incel community itself, because the community itself provides a sense of belonging that Incels do not feel outside of it. The community thus makes itself imperative in the lives of vulnerable young men and in turn further removes them from the societies they were once striving to be a part of.

In conclusion, it is important to understand that the ‘problem’ with Incels should not be targeted on the individual Incels themselves, and more on the Incel ‘community’. By applying a preventive measure in emotionally empowering young men, one could bridge the gap for them to express emotions and troubles in semantic categories other than anger. Should that fail, practitioners should be advised their P/CVE activity to re-integrate these young men in pro-social and supportive communities. Furthermore, police and local authorities need to broaden their understanding of both the technical and social aspects of Incel communities. The consequences to not doing so, as history has unfortunately shown, can be profound.

Christian Mogensen is a specialist consultant with Center for Digital Youth Care (Denmark), with responsibility for online communities, gender & sex, and destructive online behaviour.

“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.”
In our new series of podcasts, ‘RAN in Focus’, we have been exploring and dissecting some of the emerging PC/VE threats. The second in the series, released earlier this year, looked at the rising violent Incels (involuntary celibates) movement, their narratives and how they operate online. Check out this episode on the RAN YouTube channel now, soon to be available on Spotify. You watch or listen to the podcast in full here.
PROFILES:
Fabian WICHMANN
Linda SCHLEGEL
Lisa KAATI

Fabian WICHMANN
Fabian Wichmann works for Exit Germany in exit consulting and social media management, and specialises in the phenomenon of violent right-wing extremism (VRWE). He is co-initiator of the multiple award-winning initiatives Right Against Right and #HassHilft, as well as the Trojan T-Shirt. Fabian Wichmann is co-chair of the RAN Practitioners ‘Communication and Narratives’ Working Group.

Linda SCHLEGEL
Linda Schlegel is a PhD student at the Goethe University in Frankfurt and an associate research fellow at the Peace Research Institute Frankfurt (PRIF), the Global Network on Extremism and Technology (GNET), and modulisad Zentrum für angewandte Deradikalisierungsforschung. Her research interests include the nexus between gaming and extremism, (counter-)narratives, and digitally-mediated radicalisation processes.

Lisa KAATI
Lisa Kaati is a Deputy Research Director at the Swedish Defence Research Agency (FOI). Her research focuses on analysing digital phenomena and in particular threat assessments of written communication and violent extremism in digital environments.
One of the most challenging threats towards societal security is attacks from so-called violent ‘lone offenders’. These individuals are said to act alone or with minimal help from others, without any economic incitements or direct orders from violent extremist organisations. Between late 2018 and early 2020, several violent attacks in New Zealand, the US, Germany, and Norway were committed by individuals with little or no connection to extremist organisations or terrorist groups.
However, what they all had in common was that they had been active in digital environments. Fundamentally, before acting ‘alone’, these individuals were influenced either by someone, or by something, and increasingly in the online digital space.

Digital environments play an important role in inspiring, motivating, and encouraging individuals to commit violent attacks. They provide opportunities to communicate with like-minded individuals all over the world, whilst the prevalence of toxic language and conspiracy theories creates conceptions around groups of people, often stigmatising them as enemies. These conceptions subsequently serve to justify contempt, discrimination, and violence. In some digital environments glorification of violence is not uncommon and previous offenders are portrayed as inspirational role models and referred to as ‘heroes’ or ‘saints’. Indeed, some of the recent violent attacks have been preceded by manifestos published online where the perpetrators had outlined their ideology, motivation, and tactical choices.

Research shows that language generally has communicative functions beyond what is said explicitly. The way of using language reflects the author’s attitudes, personality, and emotional state. What words we use and how we express ourselves reflect both who we are and what social relationships we have. Language is the most common way for people to express inner thoughts and feelings so that others can understand. By analysing the linguistic characteristics of communication, we can understand factors that the author does not necessarily explicitly express in their text.

Thus, by analysing the perpetrators’ own words, we can learn more about them, their personality, emotional state, and how they see themselves and others. This kind of information is useful when developing methods for threat assessment in the digital space. Threat assessment takes place before an attack has been committed and focuses on detecting and preventing attacks. Threat assessment is generally carried out by law enforcement, intelligence analysts, and other security professionals.

Whilst most research on threat assessment of individuals has focused on offline settings where there is accessible information about an individual or where the individual is present and can answer questions, there is very little research that has focused on threat assessment in digital environments. Indeed, several of the common psychological factors that are considered in threat assessment in an offline setting can also be assessed in the digital space.

One of the commonly used threat assessment protocols is The Terrorist Radicalization Assessment Protocol–18™ (TRAP-18). TRAP-18 consists of two sets of variables: eight warning behaviours to identify patterns of proximal risk for intended or targeted violence and ten characteristics of lone-actor terrorists. While TRAP-18 is designed for an offline setting, some of the proximal warning behaviours and characteristics can also be identified in digital communication. The warning behaviours that are most likely to be identified in digital communication are fixation, identification, leakage, and directly communicated threats. Among the characteristics, personal grievance and dependence on a virtual community are examples of two characteristics that can be observed in digital communication.

The large amount of data that is available makes it difficult for human analysts to manually assess the threat from individuals that are active in the digital space. To assist analysts in their work there is a need for automatic or semi-automatic technologies for threat assessment that can be used as one tool in a threat assessment toolbox. While there are tools that can be used to assess the threat of an individual based on their written communication, it is still a complex problem that requires more research before it can be fully operationalised. Regardless, since digital environments have played an important role in several deadly attacks, digital threat assessment is a promising tool that can assist in preventing targeted violence.

To be able to prevent future deadly attacks we need to be more active in monitoring the digital space and identify individuals with potential violent behaviour. This means that we need apply threat assessment methods that already exist in offline communication, particularly focusing on written communication, which requires knowledge of language and ways of communicating in the fast-changing landscape of social media platforms and discussion forums.

Lisa Kaati is a Deputy Research Director at the Swedish Defence Research Agency (FOI).
A RAN Practitioners paper, published in 2021, provides practitioners with insights on how to identify digital terrorist “lone actors” before they commit violent acts, including the role and responsibilities of social media platforms and gaming platforms. The paper outlines a series of recommendations for tackling the threat. You can read the paper in full [here](https://ec.europa.eu/ran).

**Digital Terrorist & Lone Actors**

**Key outcomes**

How to find and identify digital terrorist “lone actors” before they commit violent acts was the lead question of this expert meeting. A special focus was put on the role and functions of social media platforms and gaming platforms. The term “lone-actor terrorism” has over time developed into a controversial and confusing concept. While individuals might act alone on an operational level, usually they are or feel as being a part of a specific group or movement. Particularly in the digital age, so-called “lone actors” usually are and feel neither lonely nor alone. Some “lone-actor” attackers did not join any group since they thought they would be under government surveillance, but they felt part of a collective united by shared values, actions and enemies. The trial of the Halle attacker (2020) and the Christchurch commission report (2020) indicated that neither intelligence services nor law enforcement nor the tech industry knew where to look for those digital lone actors or how to identify them online. Also, there was little awareness of the basic functionality (and abuse) of platforms, websites and other online services used by the perpetrators beyond Facebook, YouTube and Twitter.

Some of the key findings of the meeting are:

- So-called lone actors usually neither are nor feel lonely or alone. The narrative of the “lone wolf” is inaccurate and potentially harmful since it underestimates the milieus and informal networks that provide ideological, moral and sometimes logistical support to attackers.
- Look out for particular warning signs that could have indicate that an individual is moving towards violent action, such as starting to post hate speech or manifestos describing an existential threat to their in-group and justifying or calling for violence; sharing or actively seeking do-it-yourself instructions about weapons; expressing a “need to act”; ending relationships with individuals they claim are inferior due to their skin colour, beliefs, gender or other attributes.
- Funding for policy-oriented (short-term) research as well as projects that focus on the identification of digital (sub) milieus where potential digital “lone actors” might be active i.e. mapping of actors to understand international connections, look at conversations across different platforms to potentially identify “lone actors”, and to understand which prominent narratives are significant and relevant to these online actors. Research can be done in an anonymized format to identify trends and conversations across platforms.
- Keep up the dialogue with, and pressure on, social media, video sharing and online gaming companies regarding their efforts to not only deplatform terrorist content but also identify potential digital lone-actor terrorists in a proactive way. Online platforms and researchers should develop indicators to predict behaviour, including hate speech signals and see how they interact with other indicators, and to study patterns of behaviour over time, i.e. if there is an escalation of behaviours to identify lone actors through these behaviours.

Invest in structured and ongoing peer learning modules that facilitate the exchange of lessons learned between relevant actors (CSOs/researchers/government/companies).

**Relevant practices**

Some practices have been presented:

- The [2-1-1 online interventions](https://www.2to11.de) from the Institute for Strategic Dialogue is an experimental 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 extreme right and Islamist ideologies, the programme provides an opportunity for individuals showing clear signs of radicalisation to meet and engage with someone who can support their exit from hate.

The Redirect Method by MoonshotCVE implemented by Facebook and Google can serve as inspiration. The method is designed to combat violent extremism and dangerous organisations by redirecting users who have entered hate- or violence-related search queries, towards educational resources and outreach groups. A pilot of the programme was launched with delivery partners Life After Hate in May 2019 in the United States and with Exit Australia in September 2019.

The project “Good Gaming – Well Played Democracy” by the Amadeo-Antonio Foundation in Germany combines analysis of gaming subcultures from a P/CVE perspective with digital streetwork by reaching out to online gamers and to educate them about harmful conspiracy myths. The project also trains teachers, social workers and influencers on those topics.
The interplay between Islamist extremists and the violent right wing has raised fears among policy makers and practitioners about a vicious cycle of escalating tensions between extremist movements. These dynamics do not merely present a security threat, but also risks polarising societies. But this cumulative dynamic is just one piece of the pie: increasingly, reciprocal radicalisation coexists with a trend of digital violent right wing and Islamist extremist communities not just feeding off and inspiring each other, but converging into ideologically elastic online-subcultures.
This article looks at four distinct, if at times inter-related, ways in which the violent right wing and Islamist extremist movements interact with and influence each other: 1) Reciprocal Radicalisation 2) Inspiration 3) Convergence 4) Conversion.

Reciprocal Radicalisation
As our colleague Julia Ebner argued in her 2017 book ‘The Rage’ Islamist extremists and the violent right wing rely upon each other to reinforce their shared belief that a peaceful coexistence between Muslims and non-Muslims in Western societies is not just undesirable, but that violent conflict between the two is inevitable. While Islamist extremists and the violent right wing represent of course distinct movements and ideologies, they both seek to polarise societies into antagonistic, homogenous camps.

To achieve this, they aim to portray extremists as representative of wider communities that supposedly present an existential threat to the in-group. Islamist extremist groups argue that there is a ‘war on Islam’, in which Muslims are forced to take sides, while violent right wing extremist groups are spreading dystopian conspiracy theories about the ‘Islamisation’, ‘great replacement’ or ‘white genocide’. Our research at the Institute for Strategic Dialogue (ISD) has found that despite not talking much to each other, far-right and Islamists extremists talk about each other quite a lot, especially in their online-communication.

Inspiration
There are several prominent examples of extreme right communities and violent perpetrators taking inspiration from and expressing admiration for Islamist extremist movements. The 2011 Oslo attacker cited al-Qaeda as an inspiration, and praised the group’s readiness to fight and even die to achieve its goals. Accelerationist online communities supportive of the Atomwaffen Division (AWD) similarly glorified Salafi-jihadists such as Osama Bin Laden. Others among the ranks of the violent right wing even started dreaming of a ‘white sharia’ in which women, LGBT-communities and Jews would be subordinated.
Convergence

Until recently, this phenomenon seemed to be a one-way street, with the extreme right admiring Islamist extremists without the favour being returned. But this may be changing, with violent right wing or alt-right subcultures increasingly influencing Gen-Z Islamist audiences both producing and consuming content online.

While the 9/11 attacks may be a distant memory rather than a defining moment for Gen-Z Islamist extremists, they came of age during the Global War on Terror and the rise of the Islamic State. Now, a new generation of internet-savvy Gen-Z Islamists self-describing as the ‘Akh-Right’ (a play on akhi, or brother in English, and alt- in the alt-right) are witnessing and celebrating the return of the Islamic Emirate of Afghanistan.

The ‘Akh-Right’ speak in memes, drawing on alt-right favourites such as the Wojak, Pepe and Gigachad which are now a common feature in digital Islamist subcultures. They participate in producing hazy purple video edits of the Taliban, which they dub ‘mujahidwave’ an homage itself to ‘fashwave,’ a video aesthetic pioneered by far-right circles online. They use synthpop graphic design to celebrate the Islamic State, but they also use anime to deride it.

Some violent right wing activists appeared jubilant about recent developments in Afghanistan as well. While the fond sentiments towards the Taliban are of course not universally shared within the far-right, it should not have come as major surprise that some of the most extreme voices on the right would express joy over the retreat of U.S. forces and the victory of illiberal Islamist movements.

This convergence between Islamist and violent right wing audiences online hints at the ideological elasticity of a burgeoning, and current generation of Islamist supporters online. This will only become more pronounced with time, proving more difficult to understand the allegiances and enemies of these younger movements.

Conversion

Going beyond mere reciprocal appraisal, some violent extremists have even transitioned between the supposedly hostile movements. Even though conversions are not a common occurrence, there have been a number of former neo-Nazis who converted to Islam and either immediately or eventually supported extremist interpretations of it, such as Devon Arthurs, Joseph Jeffrey Brice, Sasha L. or David Myatt (who later left Islam and remains affiliated with the Satanic Neo-Nazi cult Order of Nine Angles).

The ease with which some of these individuals transitioned between supposedly hostile ideological movements could suggest that what attracts individuals to different violent extremist movements is ultimately similar. While they may lead to different outcomes after someone has adopted a specific world-view, the precise ideological dogmas may not play a crucial role during the radicalisation process itself. Instead, direction from peers, seeking for a collective identity, notions of insecure masculinity, loneliness, humiliation and lack of purpose are among the alternative factors that could help explain the desire to take up violent extremism, independent of the specific movement. In the context of the growing trend towards ideologically elastic extremist online-subcultures, considering these alternative factors within radicalisation processes will be of increasing importance.

While the research into the online and offline interplay between violent right wing, alt-right and Islamist movements is nascent, there is an urgent need to better understand the ideological leanings of Gen-Z Islamists before they become mainstream, like their alt-right predecessors.

Jakob Guhl is Policy & Research Manager at the Institute for Strategic Dialogue (ISD), where his research focuses on the far-right, Islamist extremism, hate speech, disinformation, and conspiracy theories.

Moustafa Ayad is the Executive Director for Africa, the Middle East and Asia (AMEA) at ISD, where he monitors and tracks extremist group activity online.

Julia Ebner is a Senior Research Fellow at ISD, specialising in far-right extremism, reciprocal radicalisation and European terrorism prevention initiatives.
Highlights: RAN Activity on Emerging Threats

To participate, get involved or simply find out more information about RAN Practitioners’ work on emerging threats, please find further information below.

Due to the COVID-19 pandemic the foreseen activities will take place online. The insights and outcomes gathered from these meetings will be published in the RAN Practitioners Update and on the RAN website.

Stay tuned for updates on RAN social media channels.

For more information about RAN Practitioners activities please visit the Calendar on the RAN website here.

---

RAN Mental Health Working Group
‘Mental Health practices and interventions in PCVE’

The aim of the meeting is to share and implement existing knowledge and practices relating to PCVE and mental health.

RAN Local Working Group
‘How to best use local crime prevention approaches for PCVE’

The aim of the meeting is to discuss how practitioners can help to enable a multi-level approach in local communities for PCVE, working with local coordinators, local police, education authorities and community groups.

RAN Local Working Group
Dealing with the changing landscape of polarisation, radicalisation and extremism.

The aim of this meeting is to discuss the challenges in dealing with the current dynamics and how to further develop local strategies to be more flexible and suited to the changing landscape.

Small-scale meeting
Returning FTFs: exploring post-conflict reconciliation.

The aim of this meeting is to discuss to what extent reconciliation methods can be applied to returning FTFs in Europe.
LIBRARY: DISCOVER MORE

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 (2021)
- 'Contemporary manifestations of violent right-wing extremism in the EU: An overview of P/CVE practices'

RAN (2021)
- 'Conspiracy theories and right-wing extremism - Insights and recommendations for P/CVE'

RAN (2021)
- 'The gamification of violent extremism and lessons for P/CVE'

RAN (2021)
- 'Small scale meeting - Violent Incels and Challenges for P/CVE'

RAN (2021)
- 'Small scale meeting - Digital Terrorist and 'Lone Actors'
This publication has been commissioned by the European Commission and has been prepared by REOC Communications on behalf of RadarEurope, a subsidiary of RadarGroup.