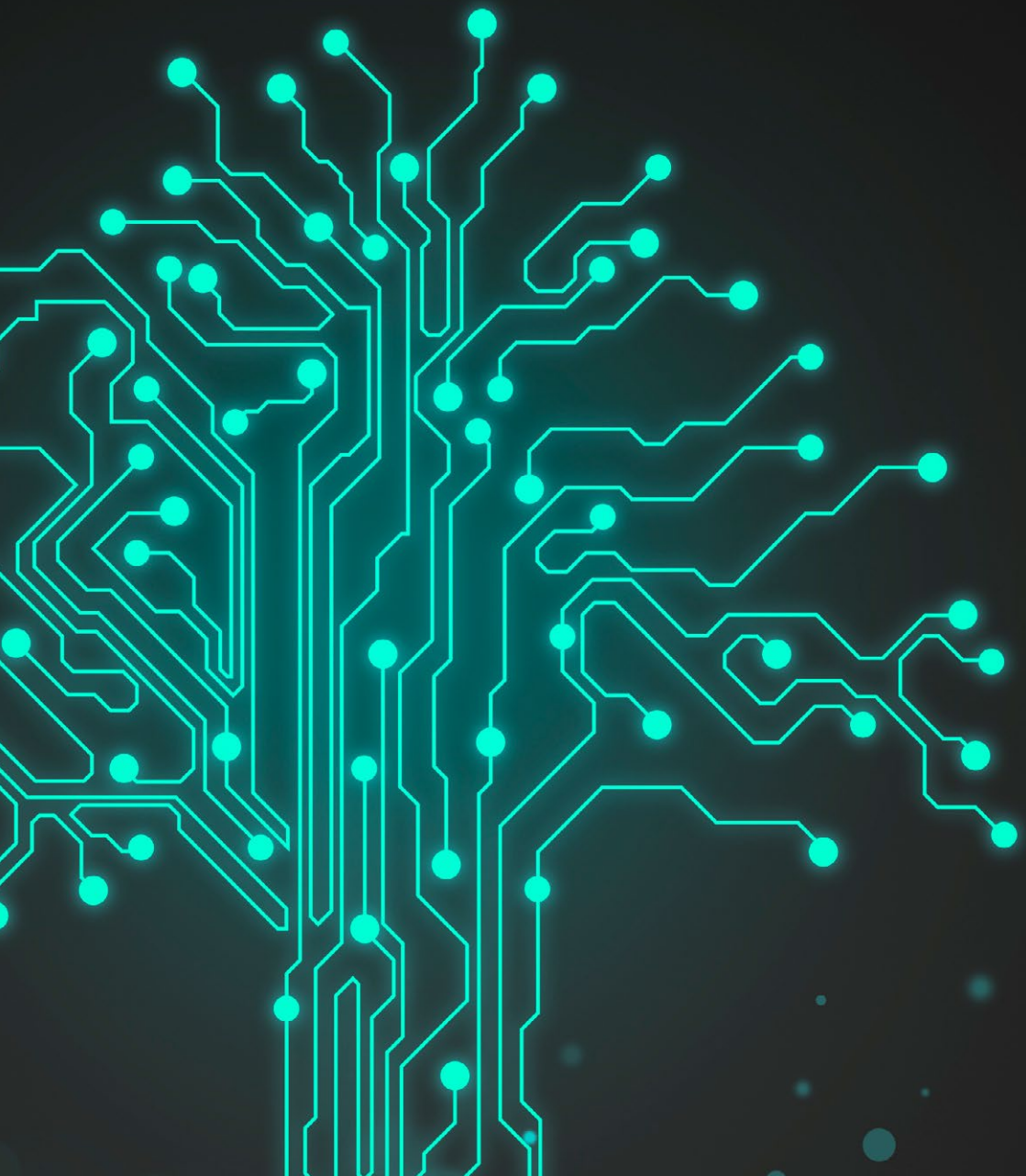
SPOTLIGHT

MARCH 2022

Digital Ecosystem



10 YEARS OF RAN

CONTRIBUTORS

Anne CRAANEN

Annukka KURKI

Carys WHOMSLEY

Charley GLEESON

Frank SIKKINK

Linda SCHLEGEL

Rachel FIELDEN

Tom DREW

Viktoras DAUKSAS

EDITORIAL

OVER the last decade or two, the world has undergone a digital transformation. In this time, terrorists and extremists have adapted to the new realities quicker than we have been able to respond. With the introduction and adoption of new digital technologies and platforms, people, both young and old, are spending more and more time online than ever before. With mobile telephony, AI, virtual reality and much more, no longer can we draw a division between online and offline. This division is becoming increasingly porous.

The Covid-19 pandemic, which ceases to abate, has accelerated this transformation and the challenges it poses. Vulnerable audiences are spending more time on news sites, social media channels, video gaming platforms and chat rooms. As a result, they are more easily targeted by terrorists, extremists and other mal actors who proliferate large amounts of disinformation, fake news, conspiracy narratives, extremist propaganda, hate speech and much more. These audiences must discern between what is real and what is fake, what is true and what is false.

As a result, the digital ecosystem is becoming both ever more complex and therefore equally important for practitioners to understand. It is one within which vulnerable audiences spend time, socialise and consume information, within which terrorists and extremists radicalise and recruit, and within which practitioners must do their work.

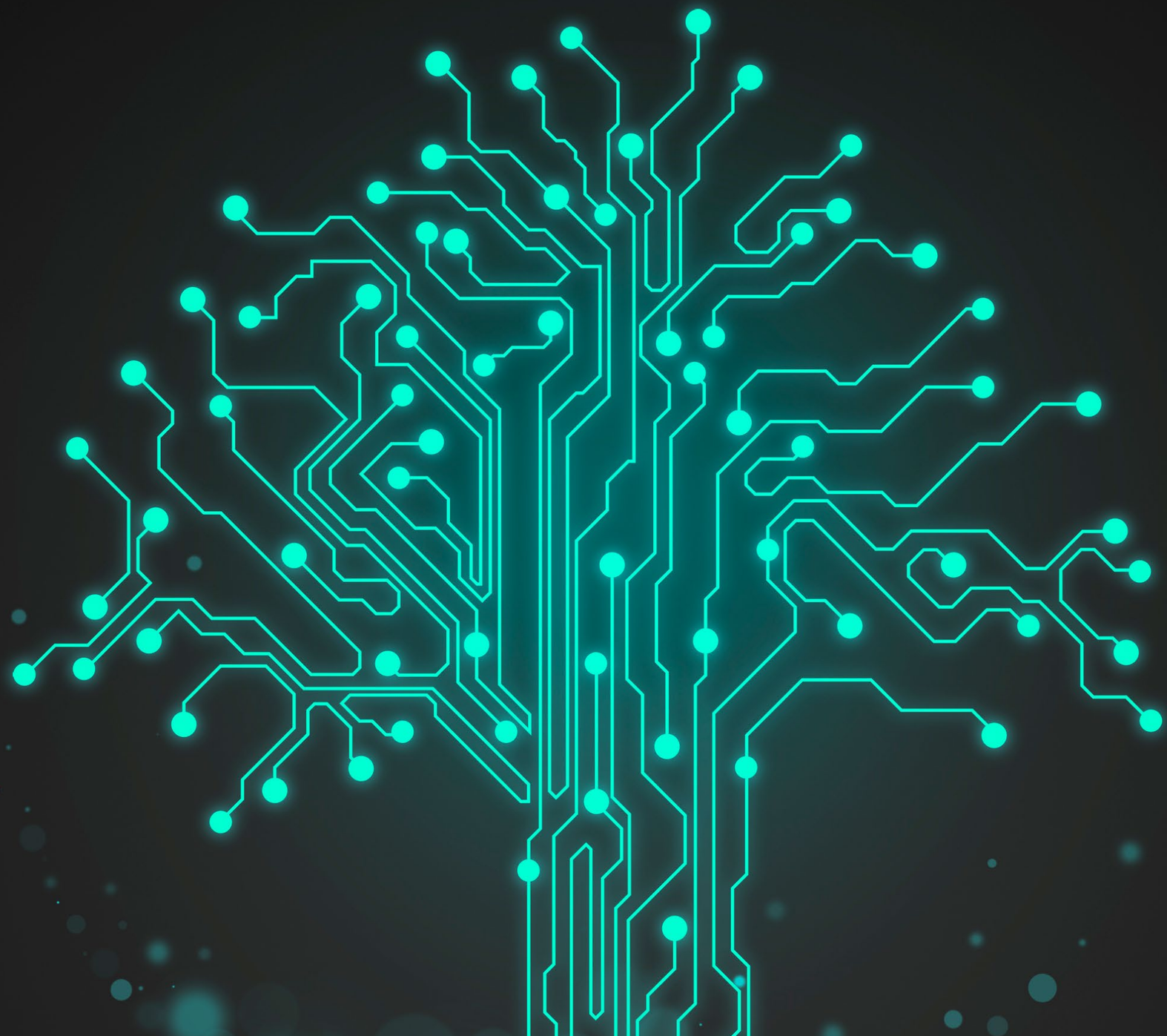
In this Spotlight, RAN practitioners and experts from outside of the network, share their insights on the digital ecosystem, and their work in addressing some of the digital challenges it presents. This Spotlight includes content on improving the digital literacy of both young people and adults, building their resilience to disinformation and conspiracy narratives, and protecting them against it.

Many of these topics have been addressed by RAN Practitioners through Working Group meetings and other activities in 2021, and will be further explored in 2022. This Spotlight publication captures the highlights from some of these activities and points practitioners to where they can read and find out more.

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**

Contents

SPOTLIGHT
CONTENTS



ARTICLE: **SPEAKING IN CODE**

Carys WHOMSLEY

PROPELLED by the global COVID-19 pandemic, many aspects of life are now taking place online. With this shift, people are increasingly reliant on social media channels to stay up to date with news and events, tackle boredom and keep in touch with friends and family. All the while, these platforms have remained highly prone to manipulation by groups looking to amplify malicious content.

Anonymity is cheap and easy to achieve, enabling the creation of convincing false online identities. These are often deployed in conjunction with the automated creation of large networks of fake accounts, to boost or lend credence to a specific message.

Empowered by automation and anonymity, hostile actors are effectively exploiting mainstream social media platforms in large scale influence operations, leveraging their artificial influence to distribute disinformation, conspiracy theories, extremism and hate.

In response to the proliferation of deceptive information online, social media giants such as Facebook and Twitter have stepped up platform moderation to curb the amplification of damaging narratives.

The popularity of fringe platforms has since grown among conspiracy theorists and extremist groups. Networks such as Telegram, Odysee and BitChute are attracting subscribers migrating towards forums in which hateful and harmful speech can be shared within narrow sets of like-minded people, concealed behind protected channels.

Yet the social media giants remain key to the dissemination of such content, and recruitment to the fringe forums. The Meta platforms, as well as YouTube and Twitter, have an enduring hold over the social media userbase distribution worldwide, hosting openly accessible profiles and trending content features. These can facilitate the reach of any narrative to the widest possible audience.

Evading Detection from Platform Moderation

Despite stringent clampdowns imposed by mainstream platforms to reduce the spread of hateful and deceptive content, bad actors carrying out coordinated inauthentic campaigns are continually devising ways to circumvent detection from the groups relying on AI trawling technologies to identify harmful content.

These ever-evolving methods include linguistic tactics. In response to violent clashes between Israel and Palestine in 2021, social media users across the Middle East adopted dotless Arabic to escape detection and censorship across Facebook, Instagram and Twitter. While this was used by authentic users wishing to express their views, such methods could be deployed by malicious groups – allowing them to hide in plain sight and influence their desired audience unhindered.

Meanwhile, the use of coded language to evade moderators across the major networks is rising. Anti-Vax groups have continued to multiply across social media platforms, for example, by coding vaccinated people as “swimmers”, and using deliberate misspellings – “wax seen” for vaccine, “Seedy Sea” for the CDC.

Other visual tactics have also been used in numerous online harassment campaigns. In September 2021, emojis were revealed as a significant stumbling block in online moderation, with tech giants slow to identify racist abuse using emojis on their platforms. Emojis of money bags, for example, were linked to anti-Semitic posts.

The benefits of this type of platform manipulation are twofold. Coded speech can allow harmful content to maximise its online lifespan, providing the means for hostile actors to infiltrate or establish online communities made up of vulnerable audiences. At the same time, the adoption of a secret language can tighten the bonds of the community – building trust, and providing a way to mark themselves as being a part of the ‘in the know’ subculture.

The Drawbacks of Ciphers

While the constant conception of new methods to evade detection may seem discouraging, the existence of the issue is evidence that moderation is effective. Through diligent monitoring, these codes can be identified and folded into existing detection software – and as soon as an identified code is incorporated into detection tools, its use will be short lived.

Moreover, as the language used by malicious groups to evade detection becomes more cryptic, the less accessible it will become to their target audience. If social media users happening upon new codes are confused about their meaning, these are unlikely to take hold. With dedicated efforts to find and incorporate new codes into detection technologies, such ciphers will become increasingly obscure - and the days of detection-evading techniques through language may be numbered.

Carys Whomsley *is an Associate Director and Head of Research and Thought Leadership at Digitalis, specialising in cross-border investigations for international disputes. Carys has led numerous investigations into online disinformation campaigns targeting individuals and organisations, enabling the identification of hostile anonymous actors carrying out sophisticated attacks, and supporting actions to limit their impact.*

“While the constant conception of new methods to evade detection may seem discouraging, the existence of the issue is evidence that moderation is effective. Through diligent monitoring, these codes can be identified and folded into existing detection software.”

RAN PRACTITIONERS PODCAST

The latest episode of RAN Practitioners' podcast series, 'RAN in Focus', takes a look at the impact of technology in P/CVE. The programme discusses the rise of conspiracy narratives, the digital networks used by terrorists to radicalise vulnerable individuals, and the adoption of technology by practitioners to connect with vulnerable individuals and with each other. The podcast hears from three experts working in tech, including Anne Craanen from Tech Against Terrorism, Joshua Fisher-Birch from the Counter Extremism Project, and Ross Frenett from Moonshot, and Working Group lead for the Communications and Narratives Working Group. You can listen to the podcast in full **here**.

PODCAST
TECH IN P/CVE

MARCH 2022
DIGITAL ECOSYSTEM

ARTICLE: **THE SMARTPHONE GENERATION**

Frank SIKKINK

IT IS 2022. The COVID-19 pandemic still grips the world. It holds people in its grip, adults and certainly also young people. Now that the end of lockdowns and restrictive measures in many countries within Europe is finally in sight, it is good to look at where we are now with regard to the well-being of young people. And there are some startling facts.

“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.”

Schools tried to ensure that students remained in control of their studies, but were not always able to organise this properly. School kids sometimes had only one moment in the day to interact with their teacher online. The lockdowns also emphasised that not every child gets the same opportunities to work on their talents, receive good education and achieve sufficient results for further education. The lockdowns have left us with a generation that has not been able to motivate itself to both attend classes all day and do homework. As a result, many young people did not pass their exams. In addition, it appears that the complete lack of physical contact with peers has made young people even more susceptible to the world of digital algorithms.

The neighbourhood that is most important to young people is the online neighbourhood. The smartphone and social media platforms are the (only) way to stay in touch with all of their friends. Government-imposed lockdown restrictions and the lack of mainstream education mean that young people have become more dependent on their phones and social media for their social environment.

Figures show that adults use on average around four to five different online platforms. In the Gen-Z generation (15-25 years) there are no fewer than 8.4! For many professional social workers and youth workers many of these platforms are not well known or understood. The task therefore is to provide these professionals with more knowledge and insights about the platforms being used so that they can carry out their work in an effective way.

The world is also becoming increasingly polarised. Both the COVID crisis and the climate crisis are testament to this. The importance of this is something that also depends on the filter bubble you are in. If we adults are no longer aware of this filter bubble, how can we support our new generations in this.

The world is also becoming more and more hi-tech. Mobile penetration and usage is at an all-time high. Younger generations

know of no other means to connect one-to-one than through a small smart device. It determines the route you take to get somewhere, it determines your (political) preference, it proposes who your friends could be, it determines… your life.

As a youth and media specialist and former youth worker, I certainly see the benefits of social media. However, I am also concerned about the web of algorithms that influence young people. Can they still discover themselves, investigate for themselves where the route leads, find out for themselves which (political) side you want to take, get to know new friends through conversation and meeting, determine their own life?

Local youth workers and social workers can help young people on many fronts. They can help spread factual messages to counteract the abundance of fake news, or talk to them if they are spreading incorrect information. This is more helpful than discussing the subject at the late night talk show tables on TV. This generation hardly ever watches TV.

It is also a huge opportunity for youth workers to make young people more media literate. Collaboration with schools is a win-win situation in this regard. Schools meet the social wishes to (better) guide young people in online activities. On the other hand, the youth workers are clearly visible to the young people when, for example, they provide lessons on media literacy in schools. They can also digitally connect with young people, who can then approach the professional again. If they want to participate in an activity or if they have problems that they do not (want to) discuss with their parents.

Youth workers/social workers need to get, (and stay) in touch with young people, both offline and online. When they see comments and posts online from young people they know they need to be able to respond. Online (youth) work is a crucial aspect of contemporary youth and social work.

We must take care of each other, especially in difficult times. We must maintain contact with the younger generations by any means necessary. Digital youth work can help to offer young people an extra opportunity to interact, with a low threshold, with a professional they 'know'. Youth workers and social workers can help tell real stories and facts (about the pandemic), see and hear (mental) problems and be the first helping hand. Recognising and signalling interest in more extreme ideologies is of course also very valuable in preventing (possible) violent incidents. The use of certain emojis can already indicate the adherence to a certain ideology. Here too, good online work can be the first step and possible problems can be prevented.

In order to realise this, policy makers need to be aware of the importance of working digitally. It is not something that professionals do in addition to their normal activities. Working well online takes time, good equipment, training and support!

Frank Sikkink *is a specialist in online youth work and the impact of social media on children, teenagers and youngsters. He provides training on all related topics such as cyberbullying, sexting, polarisation and hate speech.*

FEATURE

DETECTING MANIPULATED IMAGES

DISINFORMATION is most commonly characterised as the spread of false statements and written information on social media and peer-to-peer messaging platforms. Armed with enough ‘ground truth’ information, it is easy for moderators to spot and take action against.

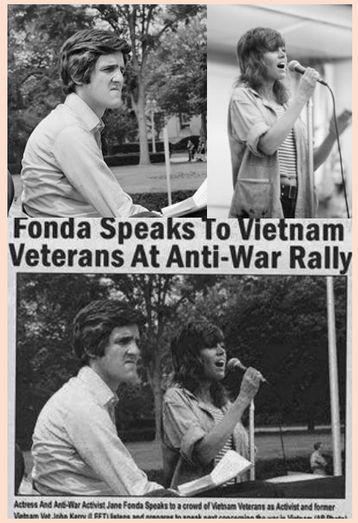


IMAGE 1

Faculty’s work in disinformation analysis has found it is far harder for humans to determine whether a high-quality manipulated image is real or fake and that digitally altered imagery and video can be far more convincing in the promotion of disinformation than statements on social media.

The use of manipulated imagery for political disinformation is almost as old as the photograph itself. Tampered photography was extensively used by both Axis and Allied powers before and during the Second World War to promote disinformation and has been used on social media by supporters from across the political landscape in every major Western election in recent history.

Image 1 is an example from the 2004 US election, in which Republican supporters attempted to stir up controversy over candidate John Kerry’s service during the Vietnam war, seeking to portray him as a pacifist and undermine his military service and awards. They did that through creating a fake image allegedly showing him at a rally with actor and anti-war campaigner Jane Fonda (right). As the two images on the left show, this is a composite of images from completely different contexts.

Image editing technology has evolved considerably over the past decade, driven by the huge growth in popularity of image and video sharing online platforms. It is now possible to make faked images of professional quality that previously would have taken considerable resource to produce, using just a mobile phone.

But just as the technology to produce sophisticated fakes has evolved, so has our ability to develop technology to detect and analyse them.

At Faculty, we have developed proprietary technology that allows us to not only detect whether or not an image has been tampered, but also highlight exactly where in the image the forgery has taken place.

Our artificial intelligence is able to analyse the entire processing history of any image that is shown. That processing history includes everything that has happened to get an image from the real world onto a computer. That includes information about the camera that captured the image, any editing in photoshop, any effects of compression caused by saving the image (and so on).

We are then able to take that information to look for inconsistencies within any image we analyse, that will highlight whether and where an image has been manipulated.

In Image 2, most people looking at the image on top would not necessarily know that it had been manipulated, or be able to consistently say how it had been manipulated. But, as visualised on the image of the bottom. Faculty's artificial intelligence is able to highlight that the man wearing the green t-shirt has been spliced into the image, as the processing history for that part of the image appears to be inconsistent with that of the rest of the image.

In this respect, artificial intelligence has grown from a tool that is useful for supporting human decision making to one that, in some cases, can now outperform humans in its ability to spot falsified content.

Faculty is currently deploying this technology with Governments and law enforcement agencies across the world as part of a suite of artificial intelligence technology we have developed to support better analysis of disinformation, falsified and harmful online content.

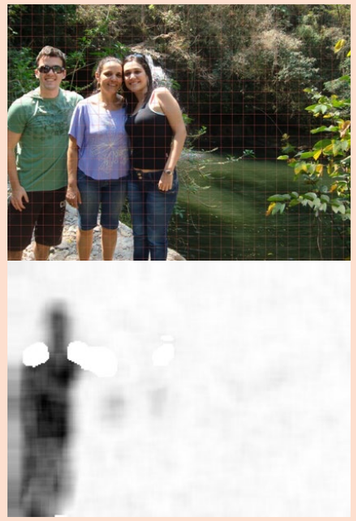


IMAGE 2

"Faculty is currently deploying this technology with Governments and law enforcement agencies across the world as part of a suite of artificial intelligence technology we have developed to support better analysis of disinformation, falsified and harmful online content."

Faculty is a leading technology company based in London which provides software, consulting, and services related to artificial intelligence. For more information, please contact **tom.drew@faculty.ai**

PROFILES: **Annukka KURKI**

Veera TUOMALA

Annukka KURKI

ANNUKKA Kurki is a member of the national working group on P-CVE and works as a Project Developer at Save the Children Finland. Her primary focus is on RadicalWeb, a project that aims to prevent radicalisation and violent extremism in young people. Annukka holds a Master's degree in International Politics and Security Studies from the University of Bradford, UK and in Development and International Cooperation from University of Jyväskylä, Finland. Her professional interests lie specifically in P/CVE, peacebuilding and peace education. She has gathered expertise in these thematic areas by working with various national and international organisations, such as Finn Church Aid, African Centre for the Constructive Resolution of Disputes (ACCORD), and the Ministry for Foreign Affairs of Finland.

Veera TUOMALA

VEERA Tuomala is a member of the national working group on P-CVE and works as a P/CVE Advisor and Project Developer at Save the Children Finland. Her 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. Veera holds a Master's degree in Security Studies from University College London and has worked in various international organisations and NGOs – including the UN and OSCE.

A paper, published by RAN Practitioners in March 2021, entitled 'Digital Exit Work', provides practitioners working in the field of exit work with insights and guidance on how to reach and engage vulnerable individuals through digital platforms, including those who do not wish to engage with exit counsellors. You can read the paper in full **here**.

Radicalisation Awareness Network
RAN Practitioners

Webpage: ec.europa.eu/ran

twitter | facebook | linkedin | youtube

22/03/2021

CONCLUSION PAPER

RAN small-scale meeting on *"Digital Exit Work"*, *15 March 2021, 15:00 to 18:00 CET, online*

Digital Exit Work

Key outcomes

The effectiveness of preventing and countering violent extremism (P/CVE) interventions is based on an in-depth understanding of the relevant target audiences, and in particular of the needs of individuals. Most existing exit programmes are founded around concepts of in-person interventions where trust, respect and a personal connection are seen as essential. In this context, digital platforms and tools may serve as means to establish contact and to facilitate an offline in-person meeting. Several extremist or terrorist cases in recent years, however, have shown that a segment of individuals is not interested in in-person contact, whether with fellow extremists or with exit counsellors. This expert meeting therefore discussed existing deradicalisation or exit lessons learned, as well as good practices in reaching and working with individuals only or mostly by digital means.

Some of the key findings of the meeting are:

- Target groups comprised of "digital natives", who grew up with social media, to build emotional connections might either not see or feel a difference between online and offline in terms of the value or depth of human connections, or they might prefer a digital exchange in principle. Also, individuals with social phobia or persons who seek anonymity might prefer digital formats to help them overcome stigma, shame and security concerns.
- Online exit counselling can work well if the needs of the clients are best served by using this method. An agreement over the objectives of the counselling can serve as the starting point for a process that identifies which formats and methods might be most helpful and effective. In general, providing options like online or in-person interventions, and also regarding different counsellor profiles (e.g. peers/age/gender), increase the likelihood of building trust and a safe space.
- Partnerships between exit programmes with different strengths and capacities might be a good way to make sure (potential) clients receive offers (and/or support?) that fit their needs.

- Facilitate a broader and deeper **collaboration between civil society organisations and larger (tech) companies**, for example through the EU Internet Forum, to support moving from the existing series of small digital P/CVE or exit pilot projects to a more structured cooperation between tech companies, civil society organisations and policymakers.

Relevant practices

Life After Hate's ExitUSA programme works with mental health professionals who volunteer to support their clients. The work is structured around the triangular setting, where a member of the ExitUSA team who has their own experiences of leaving violent far-right extremism is paired in a tandem setting with the mental health professional. Together they support the client with the aim of dealing with crisis, difficult experiences and difficult situations. They also work to sensitise the client towards seeking professional mental health support locally; what does mental health support look like and what does it mean to work with your experiences in a professional setting.

The redirect method, a collaboration between larger tech companies and some civil society organisations, aims at combating violent extremists by redirecting users who search for hate-related terms towards resources, education and outreach groups that might be able to offer support.

The 1-2-1 online interventions 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.

Follow-up

A structured and continued exchange between experts should explore questions like how to have difficult in-depth conversations online, how to build trust, how to optimise referral systems (like redirect), and how to identify and interact with radicalised individuals who are currently not open for disengagement or radicalisation.

Further reading

- **On how an exit intervention can be set up:** Organisations involved in exit work have to address a number of key issues across various areas: organisational structure and objectives, hiring staff and working with formers, engaging with radicalised individuals, media and communication, safety aspects and confidentiality, quality measures and evaluation, and working with returnees. This paper aims to help guide organisations in addressing these issues. It also addresses which attributes and skills make an exit worker suitable, how to engage with radicalised individuals, and how to deal with the media, confidentiality, security and evaluation.
- **On how to communicate with radicalised individuals in an exit setting:** During a RAN EXIT meeting on this topic, it was discussed that communication between practitioner and participants is one of the core elements of exit work. In the meantime, it is a challenge to establish and maintain a

ARTICLE: **ENHANCING DIGITAL AND MEDIA LITERACY**

Annukka KURKI and Veera TUOMALA

ALTHOUGH they have been around since the first newspapers were printed, fake news, disinformation, misinformation, and conspiracy narratives seem to be more prominent in our everyday lives than ever before. The COVID-19 pandemic has brought on an onslaught of new conspiracies and the spread of dangerous misinformation has been extremely worrying. The aim of conspiracies is to polarise and increase tension between people, which is why it is vital to be able to separate fact from fiction.

According to various studies, individuals who believe in conspiracies are likely to believe not just one but be susceptible to many others as well. This can make them an opportune target for extremist narratives – indeed, violent extremists have exploited the chaos caused by the pandemic. Thus, developing skills that increase one's capacity and ability to critically analyse media content and make informed decisions about what sources to trust, both online and offline, is of crucial importance. The significance of media and information literacy continues to be recognised – especially when it comes to digital environments. In 2014, UNESCO adopted the Paris Declaration on Media and Information Literacy (MIL), which calls for a renewed emphasis on MIL in digital environments, including ethical norms based on human rights.

While social media provides us with the possibility to connect with people all around the world, it has also become a breeding ground for extremist narratives and hate speech, which has only been fuelled by the infodemic brought on by the COVID-19 crisis. To counter this, it is easy to reason that regulation would be an effective solution. However, the constant evolution of both platforms and the spread of fake news makes it extremely difficult to target with regulation. The 2021 Media Literacy Index (MLI) recommends education over regulation in countering disinformation and building resilience to it. Much like a vaccine would protect against a disease, by gaining media and information literacy skills we can build resistance to fake news and post-truth.

As defined by the EU Expert Group on Media Literacy, the term includes "all the technical, cognitive, social, civic and creative capacities that allow a citizen to access, have a critical understanding of the media and interact with it". Media literacy varies substantially across Europe, with Finland leading the MLI ranking, and North Macedonia coming in last place – the difference between these countries is considerable. Nonetheless, a wide variety of projects and policies relating to MIL education are implemented across Europe, with civil society actors at the forefront. These projects focus on skills such as creativity, critical thinking, intercultural dialogue, media use, participation, and interaction, and highlight the importance of a multi-sectoral, interdisciplinary approach to media and information literacy education.

However, the practice and research of media literacy education continues to focus on children and youth – whereas adults, especially older adults, receive much less attention. Although numerous studies have been conducted to determine the level of media literacy within different age groups, it is difficult to make such comparisons. This is because media literacy is made up of a highly context and age-dependent range of multifaceted competencies. It is thereby important to enhance the media literacy of all age groups and customise learning to fit the context and needs of each age group.

Finland has ranked at the top of the media literacy index for many years. The 2019 national media policy states that "media literacy is currently held as an important element of civic competence that contributes to the possibilities of people and communities to live a good meaningful life". It is well embedded in national strategies and curriculums, and receives both private and public funding. The theme is also often discussed and addressed in public discourse, and Finns' high regard for freedom of speech and trust in the media provides support to media education efforts. Finland's approach to media literacy is multidisciplinary, cross-sectoral and collaborative with a multitude of different actors; nongovernmental organisations, educational institutes, government, municipalities, and the private sector implementing it. Media literacy educators undergo rigorous training, which helps to ensure high quality education.

Online environments are changing the way we operate socially, culturally, technologically, and politically – they even have the potential to affect conflicts and democracies and have been a driver in extremist propaganda. Navigating the vast sea of information available to us can be overwhelming at the very

least, which is why it is paramount that we educate and equip ourselves with the skills to build our resilience to misinformation. We can only do this by learning from each other and sharing our expertise across borders.

Veera Tuomala and Annukka Kurki *work for Save the Children Finland, specialising in P/CVE work among youth and online radicalisation. More information on Veera and Annukka can be found in the 'RAN practitioners' section.*

References:

Di Carlo, I. (05.05.2020). In chaos, they thrive: The resurgence of extremist and terrorist groups during the COVID-19 pandemic.
Link here

European Policies Initiative, Open Society Institute (2021). Media Literary Index 2021.
Link here

Mapping of media literacy practices and actions in EU-28, European Audiovisual Observatory.
Link here

Ministry of Education and Culture (2019). Media literacy in Finland: National media education policy.
Link here

Nordic Policy Centre (2020). Media literacy education in Finland.
Link here

Rasi, P., Vuojärvi, H. and Ruokamo, H. (2019). Media Literacy for All Ages. Journal of Media Literacy Education. 11. 1-19. 10.23860/JMLE-2019-11-2-1.

RAN PAPER
DIGITAL GROOMING TACTICS ON VIDEO GAMING & VIDEO GAMING ADJACENT PLATFORMS

A paper, published by RAN Practitioners in March 2021, entitled 'Digital Grooming Tactics on Video Gaming & Video Gaming Adjacent Platforms', provides insights for practitioners on how terrorists and extremists exploit video gaming platforms to radicalise and recruit, as well as the opportunities to use video gaming platforms in a positive way. You can read the paper in full **here**.

Radicalisation Awareness Network
RAN Practitioners

Webpage: ec.europa.eu/ran

twitter | facebook | linkedin | youtube

RAN C&N

07/05/2021

CONCLUSION PAPER

RAN C&N – Digital grooming tactics on video gaming (adjacent) platforms
15-16 March 2021, Online event

Digital Grooming Tactics on Video Gaming & Video Gaming Adjacent Platforms: Threats and Opportunities

Key outcomes

The online world is more and more a part of everyday life. Just as in the offline world, online threats and pitfalls are present that can harm people or, in this context, try to radicalise them. On the other hand, many positive and empowering things are also happening online, just as they are in the offline world. During the RAN Communication and Narratives Working Group (C&N) meeting on 'Digital grooming tactics on video gaming (adjacent) platforms', the threats were discussed, as well as the opportunities to use the online video gaming platforms in a positive way. This paper first discusses the threats regarding grooming tactics on video gaming and video gaming adjacent platforms by providing background information on different models of grooming that were shared during the meeting. The similarities and differences found between grooming for radicalisation purposes and other purposes (in particular, child sexual abuse and cults) are discussed. The second part of the paper highlights recommendations that have been made to use positive and empowering ways to prevent and counter grooming through video gaming.

The key outcomes of the meeting are:

- In different types of grooming, the groomer tries to feed on (the need for) certain **emotions of the potential victim**, e.g. loneliness, insecurities.
- On video gaming adjacent platforms, a groomer for extremism could talk to a gamer during gameplay and try to **steer the conversation towards feelings of anger**.
- **Awareness-raising campaigns** targeted at youth and their parents about grooming tactics on gaming (adjacent) platforms can help to build resilience against radicalisation.
- **Engaging role models through gaming** can also help. These could be popular gamers, influencers or offline leaders.
- Practitioners need to take into consideration the possibilities video games and adjacent platforms offer as an **online outreach tool** to reach individuals at risk of radicalisation.

Threats

As identified during the exploratory C&N meeting on Extremists' Use of Video Gaming, extremists use video games for recruitment and propaganda purposes ([1]). Two of the strategies identified during the exploratory meeting related to grooming and recruitment have been further explored during this meeting: **grooming through in-game chat**, and **grooming through gaming adjacent communications platforms**, such as Discord and Twitch.

The RAN Health & Social Care Working Group (H&SC) 2019 meeting on grooming ([2]) already identified some models and stages for grooming. Some of these have been developed in the context of other fields, like child sexual abuse, but can and are also used in the context of radicalisation as there are some similarities between these fields. Building on the findings of the 2019 H&SC meeting, some lessons learned from adjacent fields and grooming in an online context were shared during the meeting at hand. The following models were presented:

- One of the first models developed to better understand the interaction between sexual offenders and (young) victims is the **four preconditions model, developed by David Finkelhor in 1984** ([3]). This model describes the steps a sexual offender takes when committing sexual abuse:
  1. The first step is the offender's **motivation to abuse**. Several factors can contribute to this motivation (e.g. specific sexual interest, emotional congruence to children).
  2. The next step is that the offender has to **overcome internal inhibitors**. For instance, they may create a storyline in which it is acceptable to impose oneself on a victim (sometimes combined with substance misuse by the offender).
  3. Then, the offender has to overcome **external inhibitors**: how can they create a situation where there is no supervision and the offender will be alone with a potential victim?
  4. The last step in this model is overcoming the **victim's resistance**: this is the moment where grooming can take place in order to deal with the victim's potential resistance. Grooming here is described as "a process in which the older and more experienced offender uses manipulation, lies, flattery and praise, while also conferring on the victim a sense of responsibility and guilt, in order to get the victim (seemingly voluntarily) to take part in sexual activities aimed at gratifying the offender."
- A more recent model that was presented is the **model of sexual grooming by Ian A. Elliott** ([4]). By combining different theories, an integrated universal model of illicit grooming is presented by Elliott. The model is founded in control theory and self-regulation approaches to behaviour, assumes a goal-directed protagonist, and comprises two distinct phases. The first phase is rapport building, incentivisation, disinhibition and security management. The second phase is a disclosure phase in which goal-relevant information is introduced in a systematic and controlled manner in order to desensitise the target.

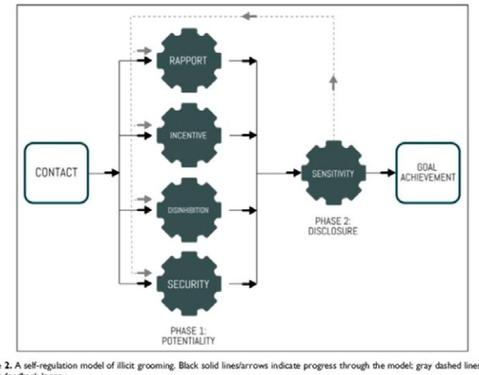


Figure 2. A self-regulation model of illicit grooming. Black solid lines/arrows indicate progress through the model; gray dashed lines/arrows indicate feedback loops.

([1]) RAN C&N Conclusion Paper, 2020: Extremists' Use of Video Gaming – Strategies and Narratives
([2]) RAN H&SC Ex Post Paper, 2019: Grooming for terror – Manipulation and control
([3]) A BRIEF SUMMARY AND CRITIQUE OF DAVID FINKELHOR'S PRECONDITIONS MODEL
([4]) A Self-Regulation Model of Sexual Grooming

ARTICLE: **READY, SET, PLAY: GAMING AND (COUNTER-) EXTREMISM**

Linda SCHLEGEL

OVER the last two years, the potential nexus between gaming and extremism has received a lot of attention. Researchers, practitioners, policy-makers and international organisations such as the EU and the UN have all declared the topic to be a key area of concern. However, surprisingly little is known about how and why extremists use not only videogames but gaming (-adjacent) platforms - such as Discord and Twitch - and gaming-related content.

The RAN Practitioners Communications & Narratives Working Group (RAN Practitioners 2020) has detailed six distinct ways both jihadists and violent right-wing extremists have sought to exploit gaming spaces:

•The production of bespoke videogames, including Hezbollah's Special Forces or the Identitarians' Heimatdefender:Rebellion game
•The modification of existing videogames, including the replication of the Christchurch attack in The Sims and Minecraft as well as the 'founding' of a white ethno-state in Roblox
•The use of the in-game chats of popular online videogames to communicate with and possibly groom (young) players
•The exploitation of gaming(-adjacent) platforms such as Steam, Discord, Twitch or DLive not only for internal communication and vetting of new recruits but to plan or stream violent actions, including the Halle attack and the January 6th insurrection (RAN Practitioners 2021a)
•The use of gaming cultural references, including the appropriation of the visual style of first-person shooter games in propaganda videos or explicit references to popular videogames such as Call of Duty
•The application of gamification – the use of game design elements in non-game contexts – in their communication, e.g. in the "achievement" section of the Halle attacker's manifesto (RAN Practitioners 2021b)

Despite the surge in recent efforts to understand the use of gaming elements and gaming-related spaces by extremists, the research gap is far and wide. Practically everything known so far about the potential nexus between gaming and extremism is largely based on anecdotal evidence and theoretical considerations. We do not know the extent of the problem, e.g. how prevalent is the presence of extremist content on gaming(-adjacent) platforms, nor whether extremists are seeking to exploit gaming-related content and spaces for reasons other than their popcultural appeal and possibilities to avoid content moderation in private groups, and also not what (if any) influence gaming has on radicalisation processes. Despite the progress that has been made in recent years, the P/CVE field as a whole is currently flying blind on most important questions regarding gaming and extremism.

The recently established Extremism and Gaming Research Network (EGRN) is seeking to turn on the proverbial light and contribute to filling the current research gap with more systematic and evidence-based analyses. While this is a much-needed effort and will ensure that P/CVE actors are able to judge and manoeuvre this emerging trend more effectively in the long-run, prevention and intervention efforts cannot wait until the (often) time-consuming research has been carried out. We may not know the extent or the exact reasons for extremists' presence in gaming spaces, but we do know that they seek to utilise these spaces, which makes gaming a relevant avenue for P/CVE.

So far, the number of projects, which have included a gaming dimension is minimal. In addition to theoretical recommendations on how to incorporate gaming in P/CVE interventions (modus | zad 2021), a certain degree of bravery and willingness for trial-and-error approaches is necessary to advance P/CVE to the gaming sphere. In other words, to prevent us from flying blind longer than necessary and possibly missing a window of opportunity to build gaming into prevention projects while extremists are still active in the space, P/CVE actors need to start using gaming content now. Without the practical insights gained from such projects, the discussion will remain largely abstract. The six ways in which extremists seek to exploit gaming-related content and spaces could serve as a starting point for the inclusion of gaming in P/CVE: Each of the six components of the typology could be used in efforts to prevent extremism just like they are apparently used for the promotion of extremism.

Despite clear evidence that extremists are seeking to exploit the gaming ecosystem, a moral panic - akin to the discussion on violent videogames and school shootings in the 1990s – is to be avoided when beginning to design projects. There is no evidence

to suggest that gamers are inherently more susceptible to radicalisation than any other group. Nevertheless, engagement with and application of gaming-related insights and content is likely to be fruitful for P/CVE not only to counter extremists' presence and action in gaming spaces but to take advantage of the immense popcultural appeal gaming holds.

Linda Schlegel *is a PhD student at Goethe University Frankfurt (Germany), a research fellow at modus | zad – Centre for Applied Research on Deradicalisation, and an associate fellow at the Peace Research Institute Frankfurt (PRIF). Her research focuses on digital radicalisation, counter- and alternative narrative campaigns, storytelling, and gaming and extremism.*

References:

EGRN
Modus | zad – Centre for Applied Research on Deradicalisation (2021)
Link here

Working Paper 1/2021: The Role of Gamification in Radicalization Processes
Link here

RAN Practitioners (2020) Extremists' Use of Video Gaming – Strategies and Narratives
Link here

RAN Practitioners (2021a) Extremists' use of gaming (adjacent) platforms – Insights regarding primary and secondary prevention measures
Link here

RAN Practitioners (2021b) The gamification of violent extremism & lessons for P/CVE
Link here

"Despite clear evidence that extremists are seeking to exploit the gaming ecosystem, a moral panic - akin to the discussion on violent videogames and school shootings in the 1990s – is to be avoided when beginning to design projects. There is no evidence to suggest that gamers are inherently more susceptible to radicalisation than any other group."

Interview: **A Day in the Life of... Viktoras Dauksas**

Viktoras DAUKSAS

SPOTLIGHT asked Viktoras Dauksas, a practitioner who runs educational media literacy campaigns in Baltic countries, Eastern Europe and the Western Balkans, ten questions about a typical day working for 'DebunkEU.org'.

What does DebunkEU.org do?
DebunkEU.org is an independent technology think tank and non-governmental organisation that researches disinformation and runs educational media literacy campaigns. DebunkEU.org provides disinformation analyses in the Baltic countries, Poland, Georgia and Montenegro, as well as in the United States and North Macedonia together with our partners.

What prompted you to set it up?
The 2014 Crimea occupation was a big trigger to start getting involved in the field of disinformation analysis.

What campaigns do you run?
The core of our work is to analyse disinformation, produce reports and communicate them. But we also do media literacy training. One of the most significant projects of 2020 was adapting the media literacy game Bad News for audiences in Lithuania, Latvia, and Estonia with more than 118 000 players trying it. The survey showed that resilience to disinformation of citizens who played the game increased 22.35 per cent.

Last year we started working with universities implementing our Civic Resilience Course, with 1000+ students testing the course: https://www.debunkeu.org/civic-resilience-course

Which campaign(s) is proving most effective, and why?
For short to mid-term impact, disinformation analysis, reporting and briefing stakeholders are very effective. Education and training are the most efficient long term solution.

How has your work changed since COVID?
It increased our workload four times. At the beginning of the pandemic it was very hard to adapt to the new realities, and to improve the process to a much bigger scale. It took around five months to manage it.

What impact are events in Ukraine and Belarus having?
The impact of these hybrid warfare events are huge. A lot of eyeballs follow these manufactured crisis. ITs use of active measures at a new scale.

What does a typical day at DebunkEU.org involve?
Analysis, analysis, analysis!
A typical day at the organisation starts with the morning cup of coffee and checking of the email box of the newsletters, concerning the latest developments in the field of disinformation. As one saying goes, 'no one can understand the truth until he drinks of coffee's frothy goodness' – hence, coffee is an essential ritual for the analyst to prepare for a debunking.

Once the morning ritual is over, the turn comes to a less cosy and attractive part which dominates the analyst's routine – reviewing and coding (or as we call it 'labelling') the information received. This is a complex and dynamic task as it requires analysts to investigate each content piece by cross-checking the factual accuracy of statements, techniques used to persuade the reader and context surrounding a particular source, author or event.

Following the analysis of the content, the analyst then proceeds with aggregating different data of the case researched and interpreting it according to the rules and practices set in this field. After that comes the writing of the report.

How important is the team of fact checkers to your work?
The field of disinformation is very broad and impacts citizens' lives. The more people and organisations work on this, the better, especially when it comes to fact checking and reporting false content.

What can we expect from DebunkEU.org in 2022?
We will keep reacting to emerging trends and expanding the scope of disinformation analysis, keeping the public and stakeholders informed about information influence operations happening across the globe.

Moreover, we will continue our work in the media literacy sphere. As the launch of the pilot version of the "Civic Resilience Course" has proven that there is a clear need for interactive solutions to increase the ability of the youth to recognise disinformation. Therefore, in 2022 we will work towards localising the course in more countries and making it accessible for students in multiple universities.

We will also continue our training-based projects. The goal for this year is to establish a Debunk Academy, with multiple programmes suited both for beginners and people practicing in the field of disinformation analysis.

How can RAN practitioners get involved?
We are open for collaboration projects and we also invite practitioners to our trainings, internship, PhD or master thesis writing or other projects. We can be contacted via our website: DebunkEU.org

IŠPŪSTI

IŠJUOKTI

MENKINTI

FEATURE

FALSIFIKU

ATRASTI

Nuo netikrų naujienų iki
so! Kiek blogio slypi
avyje? Pritrauk kiek įmanoma
daugiau sekėjų.

BAD NEWS GAME

IŠKREIPTI

PRADĖTI ŽAISTI

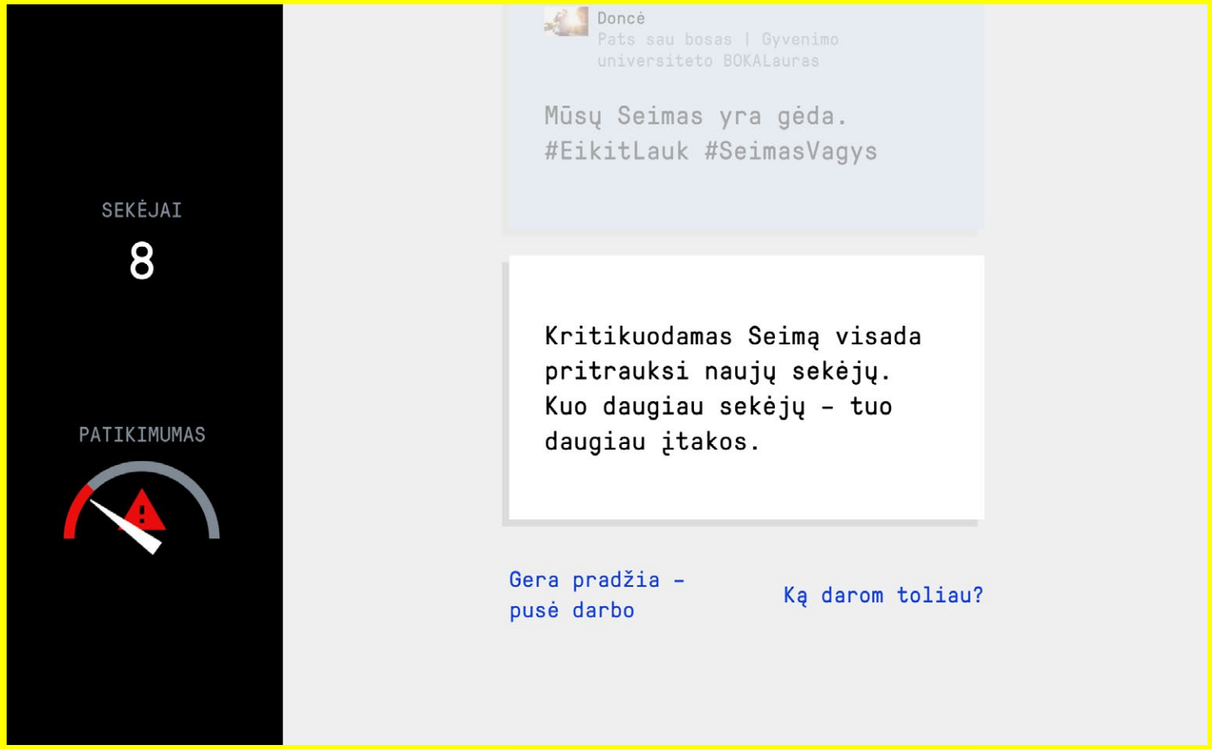
Informacija ir kitos

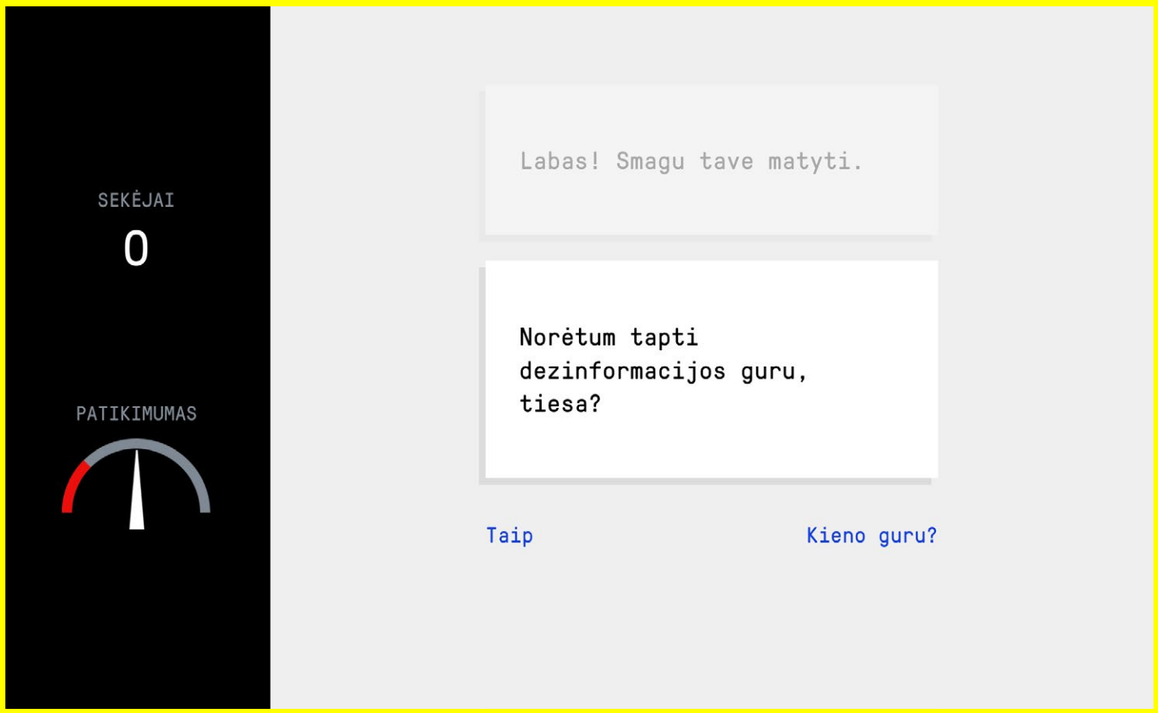
RĖKTI

INTRIGUOTI

PULTI

THROUGHOUT May-December of 2020 Debunk EU ran a media literacy project in Lithuania, Latvia, and Estonia with a goal to increase the resilience amongst the citizens of the Baltic countries through a gamified media literacy programme. The audiences in the Baltics (both local language and Russian speakers) were chosen as the target audience because the region is being constantly bombarded with false and misleading information spread by hostile sources. Moreover, a substantial part of malign content is disseminated in Russian language and is targeted to Russian minorities.





For this purpose, the Bad News game developed by the Dutch media collective DROG and Cambridge University was chosen as a possible solution to address the media literacy needs in the Baltics. It was first adapted for the local Lithuanian speaking audience in Lithuania, and then presented in Latvia and Estonia.

In total, six pages were created for the Bad News game – one for Lithuanian, Latvian, and Estonian audiences, alongside with a Russian version for each of those three countries.

The Bad News game is simple and quite straightforward: players are shown a short text or image (such as a meme or article headline) and can react to them in a variety of ways. Their score in the game is measured by followers' and 'credibility'. Choosing an option which is in line with what a 'real' producer of disinformation would do gets them more followers and credibility. If, however, they lie too blatantly to their followers, choose an option that is overtly ridiculous or act too much in line with journalistic best practices, the game either takes followers away or lowers their credibility. The goal is to gather as many followers as possible without losing too much credibility.

47 cases were selected to be adapted in the game from all three countries, choosing news stories which have received the most attention from the audiences. Local cases created a sense of reality in the game and helped showcase how easy it is to create false/misleading content online, how it is distributed, and which techniques are used to influence the audience.

To measure the impact of the project, we carried out two surveys: one general, and one of people who played the Bad News game. We compared how much the perception of credibility of the information online changed after people have played the Bad News game and found that those who did play the game started perceiving the information online more critically and did not trust it as much as they did before.

One of the most important accomplishments of the project was reaching the older generation. According to the data gathered in the end of the project, in Lithuania, 55 years and older players constituted 40 per cent, in Latvia 28 per cent, and in Estonia 35 per cent of all players.

Moreover, we have learned that the biggest impact was made amongst the younger audiences – 35.5 per cent of citizens under 34 years old in Lithuania have stated that their resilience has increased, which is a great result compared to the average of 22.35 per cent.

DebunkEU.org is an independent technology think tank and NGO that researches disinformation and runs educational media literacy campaigns. Debunk EU provides disinformation analyses in Baltic countries and Poland, as well as in the United States and North Macedonia together with our partners.

If you have any questions please feel free to contact:
Viktoras@DebunkEU.org

Find more examples of media literacy projects in the RAN Practitioners Collection of Inspiring Practices here.

“One of the most important accomplishments of the project was reaching the older generation. According to the data gathered in the end of the project, in Lithuania, 55 years and older players constituted 40 per cent, in Latvia 28 per cent, and in Estonia 35 per cent of all players.”

ARTICLE: **THE INOCULATION THEORY AND ITS USE IN COUNTERING DISINFORMATION**

Rachel FIELDEN

THE EVER-EVOLVING and adaptive nature of disinformation means that efforts to counter it have to be sustained and equally adaptable. This challenge is exacerbated by the rabbit hole effect, whereby individuals who have previously consumed and believed disinformation are more likely to believe new pieces of disinformation.

It is easy for those of us working in the field to fall into a cycle of debunk- and fact-check whack-a-mole, but these methods struggle to address the multiple, complex and interrelated falsehoods which vulnerable individuals may believe. That said, debunking remains hugely valuable. It is a core element of the broader symbiotic counter-disinformation ecosystem, much like educating people in media literacy, or arbitrator mapping and removal.

Nonetheless, we need to build resilience among groups which are vulnerable to and/or already travelling down rabbit holes of disinformation. Researchers have approached this challenge in part by studying human behaviour and psychology. In particular, by developing intervention methodologies aimed at equipping individuals with 'psychological resistance' to disinformation to break them out of a cycle of belief and provide them with long-term resilience. This work builds on inoculation theory, developed in 1961 by William J. Maguire. Maguire found that people tend to defend their beliefs by avoiding information which refutes or disproves their original beliefs, rather than actively searching for information which supports their views.

This behaviour leads to a lack of resilience and critical thinking in the face of disinformation, especially when that disinformation is communicated in a compelling way and aligns with an individual's original beliefs.

While this tendency to avoid opposing evidence and the resulting cognitive dissonance can lead a vulnerable individual into a rabbit-hole of disinformation, it can also be co-opted to build psychological resistance to disinformation. In other words, our thought processes can be protected against influence or counter-messaging through exposure to disinformation tactics.

In practice, inoculation works in four broad phases.

Phase 1 - Challenge
The subject is presented with a 'threat'. For example, a piece of disinformation that is directly incompatible with, and therefore a threat to, a factual belief held by an individual. When used as a tool in inoculation, it must be clear to the individual that the new information is a direct threat to their worldview.

E.g. "your culture is under attack" (this works best if the threat is unambiguous).

Phase 2 - Refutational Pre-emption
This is activated when an individual receives new information which does not align with their worldview, such as the example given above. This message is then paired with a refutation underlining 'the threats' weaknesses or counter-arguments.

E.g. arguments that refute the idea that "your culture is under attack" This acts as a weak 'dose' of the 'virus' which makes the individual aware of the threat of disinformation and more capable of identifying and responding to the real 'threat' in future.

Phase 3 - Delay
This is the period between the inoculation and the presentation of 'the actual threat' that is needed to process the weak version.

Phase 4 - Involvement
The subject is exposed to an actual threat (in this case extreme disinformation about immigrants) in their day-to-day.

Research suggests that, for the inoculation to work, the individual needs to care about the topic for their refutational pre-emption to be re-triggered.

In 2018, University of Cambridge researchers explored how they could develop the inoculation theory into content that was deliverable online and could encourage feelings of personal involvement with the topics at hand. They, with the Dutch media collective DROG, built a digital game called Bad News, where users played the role of propaganda producers to help them identify real world disinformation.

Games are a meaningful method of turning passive consumption into active engagement with a story or topic, ultimately leading to greater personal involvement on the part of the user. The University's gamified inoculation content was found to reduce the susceptibility to fake news headlines by an average of 21%. Similar projects include Harmony Square and Go Viral! - both great examples of how inoculation theory has been deployed in engaging formats online.

At Moonshot, my team and I developed our own game: Gali Fakta. It combines choose-your-own-adventure elements with a realistic family chat scenario. Much like real life, players are exposed by their 'family' to a range of falsehoods and other disinformation tactics. Either they will successfully separate fact from opinion and disinformation from truth, or they will be firmly but politely corrected by their cousin.

In a 2020 pilot of the game, we found that users spent 12 times as long engaging with our inoculation content when it was placed within the context of a game compared to when that same content was displayed on a website. In 2021, we began a long-term study on the impact of the game on behaviour change in relation to consumption of disinformation. In 2022, we hope to distribute the game to wider audiences.

The work undertaken by Moonshot as well as other practitioners in the industry is a part of a growing effort to build psychological resilience to disinformation while also contributing to an evidence base and in doing so, supporting global efforts to counter disinformation.

Rachel Fielden *is an analyst at Moonshot and manages its work in Indonesia.*

"In a 2020 pilot of the game, we found that users spent 12 times as long engaging with our inoculation content when it was placed within the context of a game compared to when that same content was displayed on a website."

ARTICLE: **THE OVERLAP BETWEEN TERRORIST CONTENT ONLINE, DISINFORMATION, AND THE TECH SECTOR RESPONSE**

Anne CRAANEN and Charley GLEESON

TERRORIST use of the internet is a complex and multi-faceted threat which requires an equally nuanced response. Terrorists use a wide ecosystem of tech platforms for a variety of purposes, composed of external (public propaganda dissemination) and internal (operational maintenance) communications. Our analysis shows that within the ecosystem of tech platforms there is a clear targeting of a wide range of small- and micro-platforms.

“Tech Against Terrorism believes that countering terrorist use of the internet should take a unilateral approach in ensuring that all potential avenues of terrorist exploitation are analysed so effective countermeasures can be implemented. Inter-organisation collaboration which reinforces the relationship between public and private entities should be at the basis of countering terrorist use of the internet.”

These platforms range in purpose from file-sharing, video hosting, and image sharing, to archiving, messaging, and paste sites. Tech Against Terrorism assesses that this is an issue as small tech companies do not have the capacity or capability to deal with terrorist exploitation. Therefore, we support the global tech sector counter violent extremist and terrorist use of their services whilst respecting human rights.

The use of a wide variety of platforms ensures content longevity as content removal practices across platforms have a large disparity. Large tech platforms have the capacity to build and maintain automated content moderation algorithms, whereas smaller platforms tend to lack this capability. Multiple large platforms state that over 90% of removed content is detected, flagged, and removed by automated methods, before a user is able to view it. In contrast, small- and micro-platforms rely almost exclusively on manual, human moderation which takes significantly more time in detecting and removing harmful content. Online tools like mirroring services are also being increasingly used by terrorist actors to further spread content and ensure longevity online. As such, the threat posed by online terrorist content is one that requires a collaborative and cooperative approach to effectively counter.

The evolution of terrorist content online has seen development into the realm of disinformation and conspiracy theories, especially from far-right violent extremist entities. As the lines between terrorist content, disinformation, and conspiracy theories become more blurred, content moderators operate in a grey-zone where they must determine what content meets the threshold of illegal. Some studies have shown the prevalence of conspiratorial thinking within extremism and have highlighted conspiracy theories as having a functional role in violent extremist groups. Tech Against Terrorism has noted the use of COVID-19 conspiracy theories and disinformation as recruitment tools into far-right violent extremist movements, especially highlighted by the increasing overlap between online content. Similarly, some Islamist terrorist groups have published propaganda featuring messages against vaccinations for COVID-19, stating that the virus is an act of God. The manipulation of disinformation and conspiracy theories,

especially those surrounding COVID-19, by terrorist groups is presenting a higher threat level as it is likely to be used to further recruit and radicalise into terrorist organisations.

Despite the difficulties in moderating online content, tech companies are at the forefront of disrupting terrorist use of the internet by content moderation, using both automated and manual methodologies. The Terrorist Content Analytics Platform (TCAP), developed by Tech Against Terrorism, uses a combination of human and automated Open Source Intelligence (OSINT) methods to identify and verify terrorist content. The TCAP then flags URLs containing terrorist content to tech platforms, assisting content moderators in identifying terrorist content. The TCAP has begun to bridge the gap in content moderation capabilities across a wide range of platforms by alerting verified terrorist content to moderators. Since its inception in November 2020, the TCAP has flagged over 13,000 URLs containing terrorist content to 68 platforms, 93% of this content has now been taken down.

Tech Against Terrorism believes that countering terrorist use of the internet should take a unilateral approach in ensuring that all potential avenues of terrorist exploitation are analysed so effective countermeasures can be implemented. Inter-organisation collaboration which reinforces the relationship between public and private entities should be at the basis of countering terrorist use of the internet, to ensure that responses are proportionate and appropriate to the threat. Furthermore, as shown through our transparency-by-design approach of the TCAP, we cement all our practices in the rule of law and ensure that thorough review processes are undertaken by independent reviewers.

To conclude, countering terrorist use of the internet requires the collaboration of public and private entities, to ensure that terrorist content can be swiftly removed from online spaces, while ensuring the rule of law and human rights are thoroughly upheld.

If you want to hear more about Tech Against Terrorism, sign up to the weekly digest on its website, techagainsterrrorism.org. Also follow them on Twitter @TechvsTerrorism and @TCAPAlerts. For more questions on its work, get in touch at: **contact@techagainstterrorism.org.**

Anne Craanen *is a Senior Research Analyst at Tech Against Terrorism, researching Islamist terrorism and violent far-right extremism, as well as the role of gender in terrorism. She leads the Research Team at Tech Against Terrorism and also concentrates on OSINT analysis and terrorist use of the internet. She is the policy lead on the Terrorist Content Analytics Platform (TCAP), a platform developed by Tech Against Terrorism that alerts terrorist content to tech companies when found on their platforms. Anne has an MSc in Countering Terrorism and Organised Crime from UCL and an MA in Conflict Studies from King's College London. She has previously worked at Dataminr, Artis International and the International Centre for the Study of Radicalisation (ICSR).*

Charley Gleeson *is a TCAP Analyst at Tech Against Terrorism. Charley's work on the TCAP is focused on OSINT and policy development. Charley has a background in forensic linguistics, terrorist propaganda, and the intersection of technology and the law. Charley is also employed as the team lead of the Counter Threat Strategic Communications (CTSC) team at The Counterterrorism Group, and recently graduated from a Masters degree in Terrorism and Counter-Terrorism Studies at Royal Holloway University of London.*

RAN PAPER
LONE ACTORS IN DIGITAL ENVIRONMENTS

A paper, published by RAN Practitioners in October 2021, entitled 'Lone Actors in Digital Environments' takes a look at five cases of lone actors and their online posting behaviour prior to the attacks. The paper sheds light on behaviours of lone actors in digital environments and the extent to which they were seemingly operating alone. You can read the paper in full **here**.

Lone Actors in Digital Environments

Authored by **Cathrine Thorleifsson** and **Joey Düker**, RAN External Experts

Radicalisation Awareness Network
RAN Practitioners

easy. There are also fewer social repercussions of screen-mediated activism, where hateful propaganda is produced and can be circulated fast and anonymously.

A 2019 report reveals a link between far-right online hate and violence, highlighting that registered users of Stormfront (the first far-right website founded in 1995) had murdered nearly 100 people between 1999 and 2014, 77 of which were killed by Anders Behring Breivik on 22 July 2011[24]. Breivik used the internet in all stages of his violent radicalisation, including consuming and circulating propaganda as well as parts of his attack preparations.

Breivik's manifesto revealed references to RWE subcultures and Islamophobic websites that link the European and US RWE scenes in a paranoid alliance against Islam. Breivik frequented a number of mainstream and extremist internet forums, including the anti-Islamic blog called Gates of Vienna, the website jihadwatch.org run by US white supremacist Robert Spencer, the Norwegian Document.no site and the writings of the Islamophobic blogger Peder Are Nøstvold Jensen known as "Fjordman"[25].

Since Breivik's self-radicalisation online, new digital environments have emerged that affect individual radicalisation processes[26]. A growing body of literature on political communication has highlighted the importance of social media platforms in spreading the views of RWE actors[27]. Tech-savvy extremists from a new generation born into the digital age are utilising multiple platfroms to forge communities and find social support to conduct acts of violence, including terrorism[28].

2.1 Online Platforms

In recent years, violent right-wing extremism has increasingly been characterised by young men who radicalise in transnational digital subcultures[29] and carry out acts of violence alone. The following section outlines the most relevant online forums, social media sites and live streaming technologies, both mainstream and fringe, that have been used or are still in use by RWEs, including lone actors.

Table 1: Relevant Social Media Platforms

Social Media
Facebook: The social media platform was used by the Christchurch shooter to live-stream his attack; the Poway and Bærum shooters attempted to do the same.
Youtube: YouTube can serve to normalise and amplify right-wing extremist discourse. The platform's recommendation algorithm can direct users down a "rabbit hole" – from consuming and commenting on milder to more extreme content on the platform. The New Zealand Royal Commission of Inquiry report on the Christchurch attack notes that the shooter had donated funds to the YouTube channel of Canadian white nationalist Stefan Molyneux.[30] The Bærum attacker, too, had spent a lot of time on YouTube absorbing white supremacist and antisemitic videos.
Twitch: Live-streaming platform popular within the video gaming community. The Halle terrorist livestreamed his attack here.
Telegram: A cloud-based instant messaging service. Telegram has limited content moderation policies, only banning the promotion of violence on public channels and the sharing of illegal pornographic material[31]. This made it attractive for a loose network of channels known as "Terrorgram" that distribute content glorifying RWE lone actors[32].
Gab: An alt-tech social networking service known for its RWE user base. The RWE lone actor of the 2018 Pittsburgh synagogue shooting, Robert Bowers, announced his attack on Gab.

[24] Winter, "Online Hate," 55-56.
[25] Bjørkelo, "Extremism and the World Wide Web," 42.
[26] Palmer, "How Does Online Racism Spawn Mass Shooters."
[27] Jacobs and van Spanje, "A Time-Series Analysis," 169.
[28] Singer & Brooking, "Like War," 10.
[29] Ravndal et al. RTV Trend Report 2019.
[30] Veilleux-Lepage et al., "The Christchurch Attack Report," 2.
[31] Guhl and Davey. "A Safe Space to Hate," 1.
[32] Hope Not Hate, "The Terrorgram Network."

Highlights:
RAN Activity on Digital Ecosystem

THE digital ecosystem as a topic will be addressed within a number of RAN Practitioners activities in 2022, including Working Group meetings and webinars. Due to the COVID-19 pandemic many of the foreseen activities will take place online. The insights and outcomes gathered from these meetings will be published on the RAN Practitioners website. Stay tuned for updates in the RAN Practitioners Update and on RAN Practitioners social media channels.

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

RAN Working Group meeting

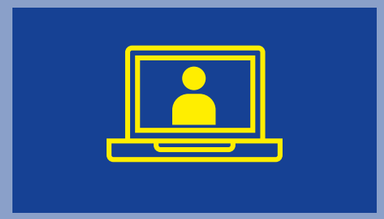
RAN WG Families, Communities and Social Care. ‘Hybrid social work and digital awareness for families’.

RAN Working Group meeting

RAN WG Rehabilitation. ‘Exploring digital/hybrid exit and rehab work’.

RAN Working Group meeting

RAN WG Youth and Education. ‘Mind the gap: How to bridge the gap between the online and offline world’.



Webinar

‘Gamification of extremism’.

Cross-cutting event

‘The online dimension of extremism and how to improve online P/CVE efforts’.

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

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 Practitioners (2021)
'Consequences of Extremist Digital Heritage on the Rehabilitation Process'

RAN Practitioners (2021)
'Digital Terrorist and 'Lone Actors'

RAN Practitioners (2020)
'How to do digital youth work in a P/CVE context: Revising the current elements'

This publication has been commissioned by the European Commission and has been prepared by REOC Communications on behalf of RadarEurope, a subsidiary of RadarGroup.