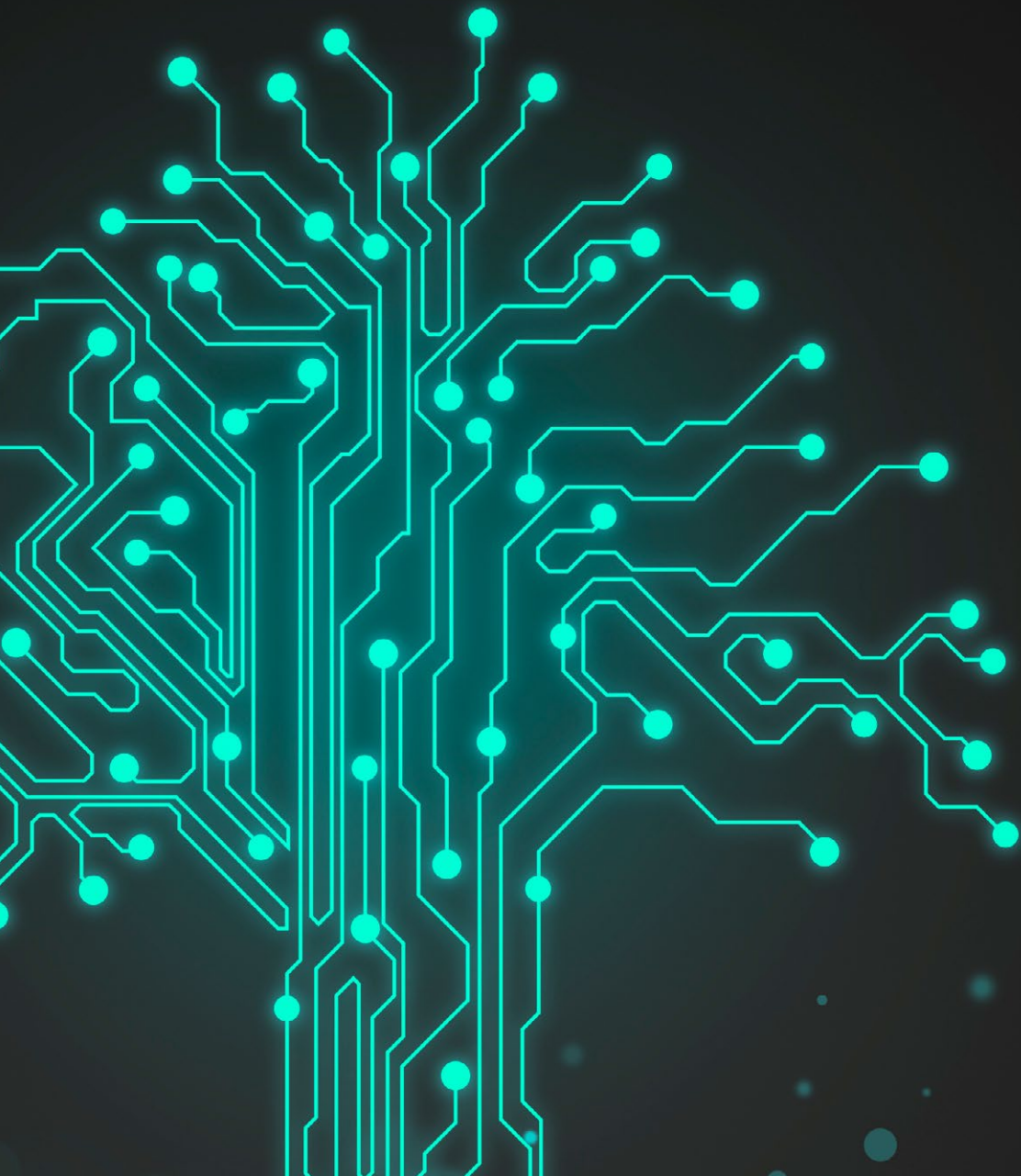


SPOTLIGHT

MAR 2022

Digitales Ökosystem



10 YEARS OF
RAN



Anne CRAANEN



Annukka KURKI



Carys WHOMSLEY



Charley GLEESON



Frank SIKKINK



Linda SCHLEGEL



Rachel FIELDEN



Tom DREW



Viktoras DAUKSAS

LEITARTIKEL

IM LAUFE der letzten ein bis zwei Jahrzehnte hat sich die Welt digitalisiert, und terroristische sowie extremistische Gruppen haben sich an diese neuen Realitäten schneller angepasst, als wir reagieren konnten. Neue digitale Technologien und Plattformen sind in Erscheinung getreten und haben sich durchgesetzt, und junge wie ältere Menschen verbringen mehr Zeit im Internet als je zuvor. Durch Smartphones, KI, virtuelle Realität und vieles mehr gehen die physische und die digitale Welt fließend ineinander über und sind nicht mehr klar voneinander abzugrenzen.

Die wieder aufflammende Covid-19-Pandemie hat diesen Wandel noch beschleunigt und die daraus resultierenden Hürden höher gelegt. Anfällige Gruppen verbringen mehr Zeit auf Nachrichtenseiten, in sozialen Medien, auf Gaming-Plattformen und in Chaträumen. Dadurch sind sie für TerroristInnen, ExtremistInnen und andere böswillige AkteurInnen einfacher zu erreichen, die in hohem Umfang Desinformation betreiben, hetzen und Fake News, Verschwörungsnarrative, extremistische Propaganda und mehr verbreiten. Diese Zielgruppen müssen zwischen authentischen und manipulativen Meldungen, zwischen wahr und falsch unterscheiden können.

Damit wird das digitale Ökosystem immer komplexer, und es ist unabdingbar, dass PraktikerInnen es durchschauen. In diesen Räumen halten sich anfällige Zielgruppen auf, sie knüpfen und pflegen soziale Kontakte und sie informieren sich; gleichzeitig radikalisieren TerroristInnen und ExtremistInnen in diesem Umfeld potenzielle neue Mitglieder und werben sie an, und PraktikerInnen müssen dort ihre Arbeit leisten.

In dieser Ausgabe von Spotlight sprechen PraktikerInnen des RAN und externe ExpertInnen über ihre Erkenntnisse zum digitalen Ökosystem und darüber, wie sie einigen der Herausforderungen entgegentreten, die die digitale Welt mit sich bringt. Diese Ausgabe beleuchtet, wie die Digitalkompetenz von jungen wie älteren Menschen verbessert wird, um ihre Resilienz gegenüber Desinformation und Verschwörungsnarrativen zu steigern.

Viele dieser Themen wurden von RAN Practitioners im Jahr 2021 durch Arbeitsgruppentreffen und andere Aktivitäten behandelt und werden auch 2022 weiter erforscht. Diese Spotlight-Ausgabe fasst einige zentrale Punkte aus diesen Aktivitäten zusammen und verweist PraktikerInnen auf weiterführende Informationen.

Wie immer freuen wir uns, von Ihnen zu hören! Wenn Sie zu künftigen Ausgaben von Spotlight beitragen möchten oder Ideen für einen Artikel, ein Interview oder ein Feature haben, wenden Sie sich bitte unter ran@radaradvies.nl an das Kommunikationsteam von RAN Practitioners.

Das Team von RAN Practitioners.

Inhalt

03

LEITARTIKEL
Digitales Ökosystem

08

ARTIKEL
Chiffren

14

PODCAST
**Technik in der P/CVE-
Arbeit**

16

ARTIKEL
Generation Smartphone

22

FEATURE
**Manipulierte Bilder
erkennen**

26

PROFILE
PraktikerInnen des RAN

28

BEITRAG
Digitale Ausstiegsarbeit

30

ARTIKEL
**Digital- und
Medienkompetenz
fördern**

36

BEITRAG
**Anwerbetaktiken in
Videospiele und auf
Gaming-Plattformen**

38

ARTIKEL
**An die Gamepads,
fertig, los: Gaming und
Extremismus
(prävention)**

44

INTERVIEW
**Ein Tag im Leben von
Viktoras Dauksas**

48

FEATURE
Das Spiel ‚Bad News

54

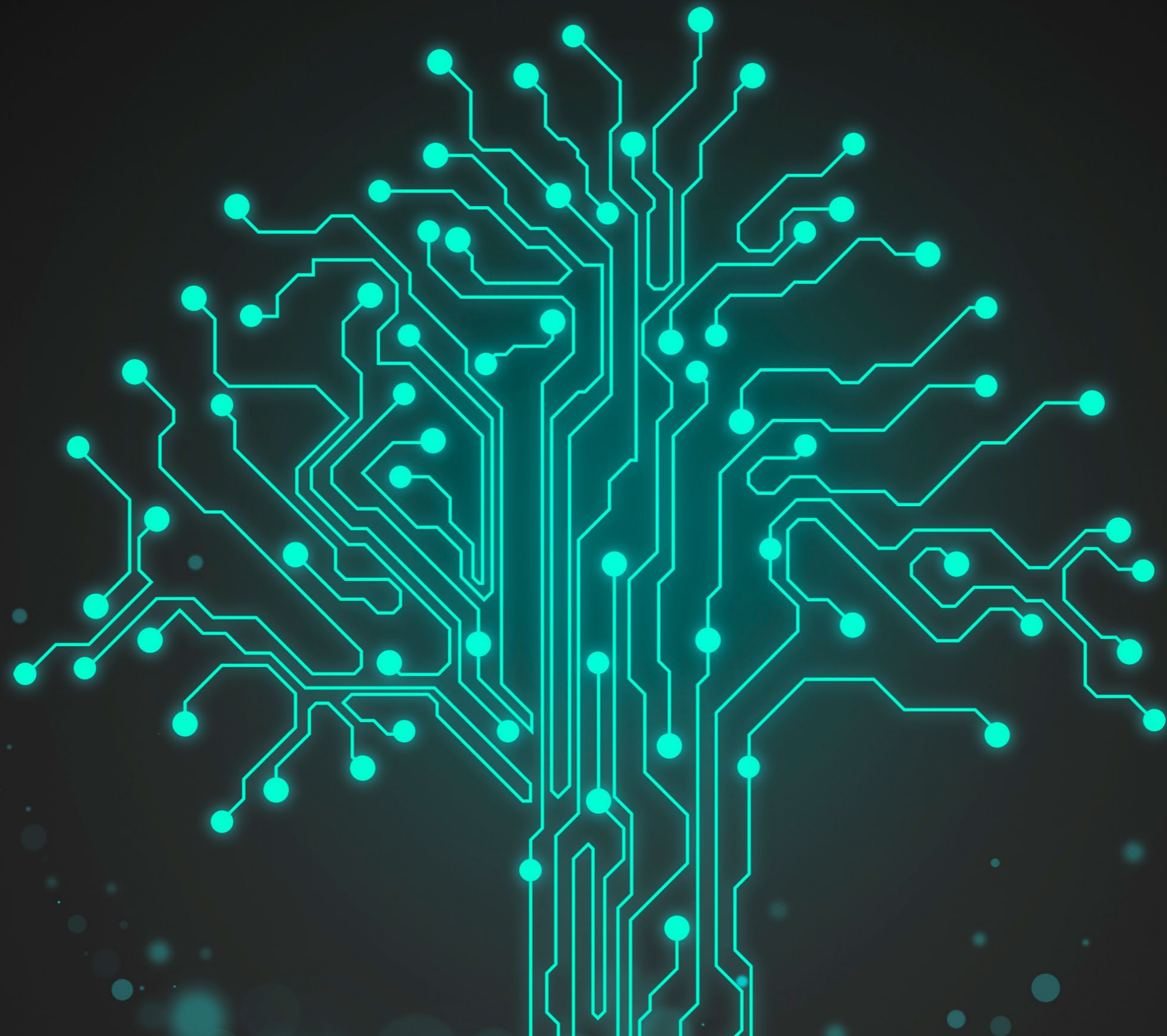
ARTIKEL
Die Inokulationstheorie

60

ARTIKEL
**Die Reaktion des
Technologiesektors**

66

BEITRAG
**EinzeltäterInnen in
digitalen Umgebungen**



ARTICLE: Chiffren



**Carys
WHOMSLEY**

ANGETRIEBEN durch die COVID-19-Pandemie haben sich viele Aspekte unseres Alltags in die digitale Welt bewegt. Mit dieser Verlagerung verlassen sich Menschen zunehmend auf Kanäle in sozialen Medien, um informiert zu bleiben, sich die Zeit zu vertreiben und mit FreundInnen und der Familie Kontakt zu halten. Seit jeher sind diese Plattformen aber auch leicht durch Gruppen manipulierbar, die ihre in böser Absicht erstellten Inhalte verbreiten möchten.

Anonymität ist einfach und kostengünstig zu erreichen, sodass sich online überzeugende falsche Identitäten konstruieren lassen. Diese werden oft in großen, automatisch erstellten Netzwerken von Fake-Accounts genutzt, um eine bestimmte Botschaft zu propagieren oder glaubwürdig erscheinen zu lassen.

Mittels Automatisierung und Anonymität können böswillige AkteurInnen beliebte Social-Media-Plattformen im großen Stil für Beeinflussungsaktionen nutzen, um Verschwörungsnarrative, Extremismus und Hass über ihre künstlich aufgebaute Reichweite in die Gesellschaft zu tragen.

Um die Verbreitung irreführender Informationen und problematischer Narrative im Internet einzudämmen, haben Social-Media-Riesen wie Facebook und Twitter die Moderation ihrer Plattformen verstärkt.

Seitdem erfreuen sich alternative Plattformen unter VerschwörungsanhängerInnen und ExtremistInnen zunehmender Beliebtheit. Netzwerke wie Telegram, Odysee und BitChute ziehen NutzerInnen an, die auf der Suche nach geschützten Kanälen sind, in denen auch von Hass geprägte und schädliche Inhalte in einer schmalen Gruppe von Gleichgesinnten ausgetauscht werden können.

Die großen Social-Media-Plattformen sind für die Verbreitung solcher Inhalte jedoch nach wie vor von zentraler Bedeutung, um neue NutzerInnen für die alternativen Foren anzuwerben. Die Plattformen des Meta-Konzerns sowie YouTube und Twitter verfügen weiterhin über die größte Nutzerbasis aller sozialen Medien weltweit, hosten öffentlich einsehbare Profile und stellen Listen der aktuell am stärksten beachteten Inhalte zusammen. Mit diesen Mitteln kann potenziell jedes Narrativ das größtmögliche Publikum erreichen.

Der Plattform-Moderation ausweichen

Obwohl Mainstream-Plattformen rigoros gegen die Verbreitung irreführender und von Hass geprägter Inhalten vorgehen,

orchestrieren böswillige AkteurInnen ihre Kampagnen und arbeiten kontinuierlich an Taktiken, um Algorithmen zur Erkennung schädlicher Inhalte zu umgehen.

Diese Methoden werden stetig verfeinert und stützen sich unter anderem auf Sprache. Nach den gewaltsamen Auseinandersetzungen zwischen Israel und den palästinensischen Gebieten im Jahr 2021 wechselten Social-Media-NutzerInnen im Nahen Osten zu punktloser arabischer Schrift, um der Erkennung und Zensur auf Facebook, Instagram und Twitter zu entgehen. Dies war zwar eine Taktik echter NutzerInnen, die über ihre Ansichten schreiben wollten, solche Methoden könnten jedoch auch von Gruppen mit schlechten Absichten eingesetzt werden, um den Algorithmus mit einfachen Mitteln auszutricksen und ihre Zielgruppe ungehindert zu erreichen.

Unterdessen werden auf großen Plattformen in der Sprache immer häufiger Chiffren verwendet, um der Moderation auszuweichen. Gruppen von ImpfgegnerInnen konnten in den sozialen Medien weiter Zulauf erhalten, indem sie beispielsweise Geimpfte als „Schwimmer“ bezeichneten oder Begriffe absichtlich falsch buchstabierten – in englischer Sprache etwa „wax seen“ für „vaccine“ (Impfstoff) oder „Seedy Sea“ für „CDC“, eine Behörde des US-Gesundheitsministeriums.

Auch auf visueller Ebene wurden in zahlreichen destruktiven Kampagnen bestimmte Taktiken angewandt. Im September 2021 erwiesen sich Emojis als besonders wirksam, um unter dem Radar der Moderation zu fliegen, während die großen Plattformen dem rassistischen Missbrauch nur langsam auf die Schliche kamen. Beispielsweise wurde das Geldsack-Emoji mit antisemitischen Beiträgen in Verbindung gebracht.

Diese Art Manipulation ist für die AkteurInnen auf Plattformen gleich von zweifachem Nutzen: Erstens bleiben schädliche Inhalte auf den Plattformen durch chiffrierte Sprache länger verfügbar, sodass Online-Communitys aus anfälligen Zielgruppen infiltriert oder aufgebaut werden können. Zweitens

kann eine gemeinsame „Geheimsprache“ die Banden innerhalb der Community stärken – Vertrauen wird aufgebaut und die Mitglieder können sich als Teil einer Subkultur aus Eingeweihten verstehen.

Die Nachteile von Chiffren

Das Aufkommen immer neuer Methoden, um der Moderation zu entgehen, mag entmutigend wirken, doch allein der Umstand, dass es diese Taktiken gibt, bescheinigt der Moderation an sich Wirksamkeit. Durch sorgfältige Beobachtung lassen sich Codes identifizieren und in die genutzte Erkennungssoftware einbinden – und sobald eine erkannte Chiffre in den entsprechenden Tools hinterlegt ist, wird sie online nicht mehr lange Bestand haben.

Und da die von böswilligen Gruppen zur Umgehung der Moderation eingesetzte Sprache immer kryptischer werden muss, wird sie auch für die Zielgruppe immer unverständlicher. Wenn NutzerInnen in sozialen Medien über eine neue Chiffre stolpern und sie nicht verstehen, kann sie ihre Wirkung schwer entfalten. Mit zielgerichteten Bemühungen, neue Codes zu finden und in Erkennungstechnologien zu berücksichtigen, müssten die Chiffren immer obskurer werden – in diesem Fall hätten Techniken, der Moderation auf sprachlicher Ebene zu entgehen, ein Ablaufdatum.

***Carys Whomsley** ist Associate Director sowie Head of Research and Thought Leadership bei Digitalis, das sich auf grenzüberschreitende Untersuchungen bei internationalen Streitfällen spezialisiert. Carys hat zahlreiche Online-Desinformationskampagnen, die auf Personen und Organisationen abzielten, in leitender Funktion untersucht. Als Ergebnis konnten anonyme AkteurInnen identifiziert werden, die komplexe Angriffe orchestrierten, sowie Eindämmungsmaßnahmen unterstützt werden.*

“Und da die von böswilligen Gruppen zur Umgehung der Moderation eingesetzte Sprache immer kryptischer werden muss, wird sie auch für die Zielgruppe immer unverständlicher. Wenn NutzerInnen in sozialen Medien über eine neue Chiffre stolpern und sie nicht verstehen, kann sie ihre Wirkung schwer entfalten.”

RAN PODCAST Technik in der P/CVE-Arbeit

Die neueste Folge der Podcasts von RAN Practitioners, „RAN in Focus“, wirft einen Blick auf die Auswirkungen von Technik auf die P/CVE-Arbeit. Wir sprechen über den Aufschwung, den Verschwörungsnarrative derzeit erfahren, über die digitalen Netzwerke, in denen TerroristInnen anfällige Personen radikalisieren, und darüber, wie PraktikerInnen sich mit diesen neuen Technologien auseinandersetzen, um sich mit anfälligen Personen sowie untereinander zu vernetzen. Im Podcast kommen drei ExpertInnen zu Wort, die intensiv von Technik Gebrauch machen: Anne Craanen von Tech Against Terrorism, Joshua Fisher-Birch vom Counter Extremism Project und Ross Frenett von Moonshot, der außerdem Ko-Leiter der Arbeitsgruppe Communications and Narratives ist. [Hier](#) finden Sie die Folge dieses Podcast in voller Länge.

PODCAST
TECHNIK IN DER P/CVE-ARBEIT

MAR 2022
DIGITALES ÖKOSYSTEM



ARTIKEL: Generation Smartphone



**Frank
SIKKINK**

DAS JAHR 2022. Noch immer hat die COVID-19-Pandemie die Welt im Griff und bestimmt große Teile unseres Alltags – dies gilt für Erwachsene und sicher auch für junge Menschen. Nun, da das Ende von Lockdowns und Eindämmungsmaßnahmen in zahlreichen Ländern Europas in Sicht ist, sollten wir Bilanz zum Wohlbefinden junger Menschen ziehen. Und einige Dinge sind durchaus bemerkenswert.

“Das Umfeld, das jungen Menschen am wichtigsten ist, ist das digitale. Smartphone und soziale Medien sind ihr (einziges) Mittel, um mit Freundinnen und Freunden in Kontakt zu bleiben. Aufgrund staatlicher Kontaktbeschränkungen und ausfallendem Schulunterricht sind junge Menschen für ihre sozialen Beziehungen mehr denn je auf ihr Handy und Social Media angewiesen.”

Schulen bemühten sich, ihre Schülerinnen und Schüler nicht den Anschluss verlieren zu lassen, konnten dies jedoch nicht immer passend organisieren. Im Schulalltag blieb Kindern oft nur wenig Gelegenheit, sich online mit ihrem Lehrer oder ihrer Lehrerin auszutauschen. Durch die Lockdowns wurde auch besonders deutlich, dass nicht alle Kinder die gleichen Möglichkeiten haben, in ihren Talenten gefördert zu werden, eine gute Bildung zu erlangen und sich eine stabile Grundlage für einen höheren Abschluss zu schaffen. Die Lockdowns lassen uns mit einer Generation zurück, die sich nicht dazu motivieren kann, ganztägig am Unterricht teilzunehmen und zusätzlich Hausaufgaben abzuarbeiten. In der Folge konnten viele junge Menschen ihre Abschlussprüfungen nicht bestehen. Zudem erscheint es so, dass der starke Mangel an physischer Interaktion mit Gleichaltrigen junge Menschen noch anfälliger für die Algorithmen in der digitalen Welt gemacht hat.

Das Umfeld, das jungen Menschen am wichtigsten ist, ist das digitale. Smartphone und soziale Medien sind ihr (einziges) Mittel, um mit Freundinnen und Freunden in Kontakt zu bleiben. Aufgrund staatlicher Kontaktbeschränkungen und ausfallendem Schulunterricht sind junge Menschen für ihre sozialen Beziehungen mehr denn je auf ihr Handy und Social Media angewiesen.

Die Zahlen zeigen, dass Erwachsene durchschnittlich vier bis fünf verschiedene Online-Plattformen nutzen. Bei der „Generation Z“ (15–25 Jahre) sind es nicht weniger als 8,4! Doch viele professionelle Sozial- und JugendarbeiterInnen kennen und verstehen viele dieser Plattformen nicht sonderlich gut. Daher besteht der Bedarf, Fachkräften diese Plattformen näherzubringen, damit sie ihrer Arbeit wirksam nachkommen können.

In der Öffentlichkeit lässt sich zunehmende Polarisierung beobachten, wie anhand der Corona-Pandemie und auch der Klimakrise deutlich wird. Wie sich dies ausprägt, ist auch abhängig von der eigenen Filterblase. Wenn wir Erwachsenen uns dieser Filterblase nicht bewusst sind, wie können wir dann nachfolgende Generationen auf diesen Effekt aufmerksam machen?

Auch neue Technologien spielen in unserer Welt eine immer größere Rolle. Mehr Menschen als je zuvor besitzen ein Mobiltelefon, und auch das Ausmaß deren Nutzung ist auf einem Allzeithoch. Jüngere Generationen kennen kein anderes Mittel der persönlichen Kontaktaufnahme als über ein kleines Smart-Gerät. Es weist einem den Weg an jeden beliebigen Ort, es unterstützt das Finden einer (politischen) Überzeugung, es schlägt passende Freundinnen und Freunde vor und bestimmt ... einfach das ganze Leben.

Als Jugend- und Medienspezialist und ehemaliger Jugendarbeiter kann ich die Vorzüge der sozialen Medien definitiv erkennen. Doch das Netz aus Algorithmen, durch das junge Menschen beeinflusst werden, versetzt mich auch in Sorge. Können sie noch sich selbst finden, eigenständig den richtigen Weg für sich entdecken, ihre (politischen) Standpunkte unabhängig festigen, Menschen durch persönliche Gespräche kennenlernen und ein selbstbestimmtes Leben führen?

Lokal tätige Jugend- und SozialarbeiterInnen können jungen Menschen bei verschiedensten Aspekten ihres Lebens helfen. Sie können geprüfte Informationen verbreiten, um Fake News entgegenzuwirken, oder junge Menschen ansprechen, die Fehlinformationen teilen. Dies ist sinnvoller, als das Thema in spätabendlichen Polit-Talkshows im Fernsehen zu behandeln, denn diese Generation sieht kaum noch fern.

JugendarbeiterInnen haben auch hervorragende Möglichkeiten, die Medienkompetenz junger Menschen zu fördern. Die Zusammenarbeit mit Schulen stellt in dieser Hinsicht eine Win-win-Situation dar: Die Schulen können ihren Anspruch erfüllen, junge Menschen (besser) über Gesetzmäßigkeiten des Internets aufzuklären, und die JugendarbeiterInnen werden wiederum sichtbar für junge Menschen, wenn sie beispielsweise an Schulen über Medienkompetenz sprechen. Sie können sich digital mit jungen Menschen vernetzen, sodass diese erneut auf die Fachkraft zukommen können, wenn sie an einer Aktivität teilnehmen oder über ein Problem sprechen möchten, mit dem sie sich nicht an ihre Eltern wenden (wollen).

Jugend- und SozialarbeiterInnen müssen mit jungen Menschen sowohl offline als auch online in Kontakt treten (und bleiben). Wenn sie im Internet Kommentare und Beiträge von jungen Menschen sehen, die sie kennen, müssen sie auch reagieren können. Die Online-Arbeit ist ein wichtiger Aspekt der heutigen Jugend- und Sozialarbeit.

Wir müssen aufeinander achtgeben, besonders in schwierigen Zeiten. Wir müssen mit allen nötigen Mitteln zu jüngeren Generationen Kontakt halten. Mit digitaler Jugendarbeit kann jungen Menschen eine weitere Möglichkeit geboten werden, auf für sie einfache Weise mit einer Fachkraft zu interagieren, die sie schon einmal kennengelernt haben. Jugend- und SozialarbeiterInnen können helfen, wahre Geschichten und Fakten beispielsweise über die Pandemie zu verbreiten, (psychische) Probleme wahrzunehmen und eine erste helfende Hand auszustrecken. Extremere Ansichten zu erkennen und offen auf Menschen zuzugehen, ist natürlich sehr wichtig, um (sich anbahnende) Gewalttaten zu verhindern. Die Nutzung bestimmter Emojis kann unter Umständen bereits auf eine bestimmte Ideologie hinweisen. Auch hier kann gute Online-Arbeit ein erster Schritt zur Verhinderung möglicher Probleme sein.

Um dies umsetzen, müssen politische EntscheidungsträgerInnen die Bedeutung von Online-Arbeit kennen. Sie ist nichts, was Fachkräfte zusätzlich zu ihren normalen Aktivitäten „nebenher“ durchführen. Gute Online-Arbeit braucht Zeit, geeignete Ausrüstung, entsprechende Schulung und Unterstützung!

Frank Sikkink ist Spezialist für Online-Jugendarbeit und die Auswirkungen sozialer Medien auf Kinder, Jugendliche und Heranwachsende. Er bietet Schulungen zu allen damit zusammenhängenden Themen wie Cybermobbing, Sexting, Polarisierung und Hassrede an.

Manipulierte Bilder erkennen

DESINFORMATION tritt heute vor allem in Form sachlich falscher Aussagen und Texte in Erscheinung, die über sozialen Medien und Messenger verbreitet werden. Gestützt auf eine solide Faktenbasis können ModeratorInnen Desinformation grundsätzlich einfach erkennen und ihr entgegenwirken.



Mit Bild 1

Bei der Analyse von Desinformation hat das Unternehmen Faculty allerdings festgestellt, dass aufwändig manipulierte Bilder für Menschen deutlich schwieriger als solche zu erkennen sind und dass Desinformation mit digital bearbeitetem Bild- und Videomaterial deutlich wirksamer betrieben werden kann als mit Aussagen.

Der Einsatz manipulierter Bilder zur politischen Desinformation ist beinahe so alt wie die Fotografie selbst. Vor und während des Zweiten Weltkriegs bedienten sich sowohl die Achsenmächte als auch die Alliierten gefälschter Fotos, um Desinformation zu betreiben, und auch in der jüngeren Geschichte haben UnterstützerInnen aus der gesamten politischen Landschaft bei jeder größeren Wahl in der westlichen Welt von diesem Mittel Gebrauch gemacht.

Mit Bild 1 versuchten UnterstützerInnen der Republikanischen Partei im US-Wahlkampf 2004 eine Kontroverse um den Militärdienst des Kandidaten John Kerry in Vietnam zu entfangen, indem sie ihn als Pazifisten porträtierten und seine Pflichterfüllung und Auszeichnungen infrage stellten. Zu diesem Zweck fertigten sie Bildmaterial an, das ihn bei einer Kundgebung mit der Schauspielerin und Antikriegsaktivistin Jane Fonda (rechts) abbildete. Wie die beiden Bilder links zeigen, handelt es sich um eine Montage aus Bildern, die in einem völlig anderen Kontext aufgenommen wurden.

Im Fahrwasser des gewaltigen Wachstums von Online-Plattformen, auf denen Bilder und Videos eingestellt werden, hat Bildbearbeitungstechnologie im letzten Jahrzehnt enorme Fortschritte gemacht. Heute können Bilder mit jedem Smartphone auf professionellem Niveau gefälscht werden, wofür vor einiger Zeit noch erhebliche Ressourcen aufgewendet werden mussten.

Weiterentwickelt hat sich jedoch nicht nur die Technologie, mit der ausgeklügelte Fälschungen erzeugt werden, sondern auch die Technik zu deren Erkennung und Analyse.

Bei Faculty haben wir eine geschützte Technologie entwickelt, die nicht nur ermittelt, ob ein Bild manipuliert wurde, sondern auch genau die veränderten Stellen markiert.

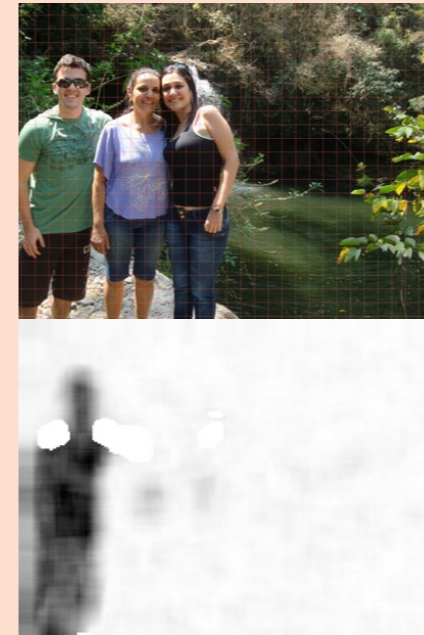
Unsere künstliche Intelligenz analysiert den gesamten Bearbeitungsverlauf eines vorgelegten Bilds. Dieser Bearbeitungsverlauf umfasst alles, was mit einem Bild geschehen ist, um es aus der Realität auf einen Computer zu bringen, einschließlich Angaben zur verwendeten Kamera, Bearbeitungen in Photoshop, durch Kompression beim Speichern erzeugte Effekte und so weiter.

Anhand dieser Daten lassen sich bei jedem analysierten Bild eventuelle Ungereimtheiten aufdecken, die darauf schließen lassen, ob und an welcher Stelle ein Bild manipuliert wurde.

Bei Bild 2 würde den meisten Menschen wahrscheinlich nicht auffallen, dass es manipuliert wurde, geschweige denn, dass sie zuverlässig sagen könnten, was damit nicht stimmt. Doch wie rechts gezeigt kann die KI von Faculty hervorheben, dass der Mann im grünen T-Shirt in das Bild montiert wurde, da die in diesem Bildausschnitt vorgenommenen Bearbeitungen nicht zum restlichen Bild passen.

Ursprünglich wurde KI entwickelt, um bessere Entscheidungen treffen zu können, doch in unserem Kontext ermöglicht sie heute Tools, die gefälschte Inhalte in einigen Fällen besser als Menschen erkennen.

Faculty stellt diese Technologie derzeit Regierungs- und Strafverfolgungsbehörden auf der ganzen Welt im Rahmen einer Suite aus KI-Tools bereit, mit denen sich Desinformation sowie gefälschte und schädliche Inhalte im Internet besser analysieren lassen.



Bei Bild 2

“Bei Faculty haben wir eine geschützte Technologie entwickelt, die nicht nur ermittelt, ob ein Bild manipuliert wurde, sondern auch genau die veränderten Stellen markiert.”



Faculty ist ein führendes Technologie-Unternehmen mit Sitz in London, das Software, Beratung und weitere Dienste in Bezug auf künstliche Intelligenz anbietet. Senden Sie für weitere Informationen eine E-Mail an:
tom.drew@faculty.ai

PROFILE: PraktikerInnen des RAN

Annukka KURKI

Veera TUOMALA



Annukka KURKI


ANNUKKA Kurki ist Mitglied der nationalen Arbeitsgruppe zu P-CVE und arbeitet als Projektentwicklerin bei Save the Children Finnland. Ihr Hauptaugenmerk liegt auf RadicalWeb, einem Projekt, das darauf abzielt, Radikalisierung und gewaltbereiten Extremismus bei jungen Menschen zu verhindern. Annukka hat einen Masterabschluss in International Politics and Security Studies an der University of Bradford (Vereinigtes Königreich) sowie in Development and International Cooperation an der Universität Jyväskylä (Finnland) erworben. Ihre beruflichen Interessen liegen speziell in den Bereichen P/CVE, Friedenskonsolidierung und Friedenserziehung. Mit ihrer Arbeit bei verschiedenen nationalen wie internationalen Organisationen wie Finn Church Aid, African Centre for the Constructive Resolution of Disputes (ACCORD) und dem Außenministerium Finnlands hat sie Fachkenntnisse zu diesen Themengebieten zusammengetragen.




Veera TUOMALA

VEERA Tuomala ist Mitglied der nationalen Arbeitsgruppe zu P-CVE und arbeitet als P/CVE-Beraterin und Projektentwicklerin bei Save the Children Finnland. Ihr Hauptaugenmerk liegt auf RadicalWeb, einem Projekt, das darauf abzielt, Radikalisierung und gewaltbereiten Extremismus bei jungen Menschen zu verhindern, indem JugendarbeiterInnen in Früherkennung und Dialog geschult werden. RadicalWeb ist Teil des aktuellen nationalen Aktionsplans zur Prävention von gewaltbereiter Radikalisierung und Extremismus. Veera Tuomala hat einen Masterabschluss in Security Studies am University College London erworben und in verschiedenen internationalen Organisationen und Nichtregierungsorganisationen – darunter die UNO und die OSZE – gearbeitet.

Radicalisation Awareness Network



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.

Product of the Radicalisation Awareness Network
(RAN)



Radicalisation Awareness Network



CONCLUSION PAPER
Digital EXIT Work
Page 4 of 6

- 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

Product of the Radicalisation Awareness Network
(RAN)



ARTIKEL: Digital- und Medienkompetenz fördern



**Annukka
KURKI
and
Veera
TUOMALA**

OBWOHL es sie bereits seit dem Druck der ersten Zeitungen gibt, sind Fake News, Desinformation, Falschinformationen und Verschwörungsnarrative in unserem Alltag präsenter als jemals zuvor. Die COVID-19-Pandemie hat eine Fülle neuer Verschwörungsnarrative hervorgebracht, und die Verbreitung potenziell schädlicher Falschinformationen ist äußerst besorgniserregend. Verschwörungserzählungen haben zum Ziel, die Gesellschaft zu polarisieren und Spannungen zwischen Menschen zu erzeugen, weshalb es unabdingbar ist, zwischen Fakt und Fiktion unterscheiden zu können.

Verschiedenen Studien zufolge sind AnhängerInnen von Verschwörungsnarrativen tendenziell nicht nur für eine bestimmte, sondern grundsätzlich für viele Erzählungen dieser Art anfällig. Dies kann sie zu einem vielversprechenden Ziel für extremistische Narrative machen, und tatsächlich haben extremistische Gruppierungen das durch die Pandemie verursachte Chaos zu ihrem Vorteil genutzt. Menschen darin zu schulen, sowohl online als auch offline Medieninhalte kritisch zu analysieren und die Vertrauenswürdigkeit von Quellen fundiert zu beurteilen, ist daher entscheidend. Medien- und Informationskompetenz wird hohe Bedeutung beigemessen – insbesondere in Bezug auf digitale Umgebungen. Mit der „Paris Declaration on Media and Information Literacy“ rief die UNESCO im Jahr 2014 dazu auf, in digitalen Umgebungen erneut einen Fokus auf Medien- und Informationskompetenz zu legen, wobei auch auf den Menschenrechten fußende ethische Normen eine Rolle zu spielen haben.

Soziale Medien ermöglichen uns zwar, mit Menschen auf der ganzen Welt in Kontakt zu treten, haben sich jedoch auch als Nährboden für extremistische Narrative und Hetze erwiesen, was sich durch die Infodemie im Zuge der COVID-19-Krise noch verschärft hat. Es liegt nahe, entsprechende Plattformen als Gegenmaßnahme stärker zu regulieren. Allerdings entwickeln sich sowohl Plattformen als auch Verbreitungsmethoden für Fake News ständig weiter, was zielgerichtete Regulierung schwierig macht. Der Media Literacy Index des Jahres 2021 empfiehlt Aufklärung anstatt Regulierung, um Desinformation wirksam entgegenzutreten und Resilienz aufzubauen. Ähnlich wie durch einen Impfstoff gegen eine Krankheit können wir durch Medien- und Informationskompetenz Abwehrkräfte gegenüber falschen, irreführenden und postfaktischen Meldungen entwickeln.

Die EU-Expertengruppe zu Medienkompetenz definiert diesen Begriff als alle technischen, kognitiven, sozialen, bürgerschaftlichen und kreativen Kompetenzen, durch die

BürgerInnen auf Medieninhalte zugreifen, sie kritisch einordnen und mit ihnen interagieren können. Die Medienkompetenz ist über Europa hinweg sehr unterschiedlich ausgeprägt – Finnland führt die Rangliste an, Nordmazedonien ist das Schlusslicht, und der Unterschied zwischen diesen Ländern ist beachtlich. Nichtsdestotrotz werden in ganz Europa verschiedenste Projekte und Maßnahmen zur Förderung der Medien- und Informationskompetenz umgesetzt, in erster Linie durch zivilgesellschaftliche Organisationen. Diese Projekte konzentrieren sich auf Kompetenzen wie Kreativität, kritisches Denken, interkulturellen Dialog, Mediennutzung, Teilhabe und Interaktion, und sie unterstreichen, wie wichtig es ist, multisektoral und interdisziplinär an die Förderung von Medien- und Informationskompetenz heranzugehen.

Forschung und Praxis in Bezug auf Medienkompetenzförderung ist jedoch weiterhin auf Kinder und Jugendliche konzentriert, und Erwachsenen, insbesondere älteren, wird kaum Aufmerksamkeit zuteil. Obwohl die Medienkompetenz innerhalb verschiedener Altersgruppen in zahlreichen Studien untersucht wurde, gestalten sich Vergleiche schwierig, denn Medienkompetenz setzt sich aus verschiedensten Fertigkeiten zusammen, die stark kontext- und altersabhängig sind. Daher sind die Förderungsansätze an den Kontext und die Bedürfnisse der verschiedenen Altersgruppen anzupassen, um die Medienkompetenz in der gesamten Gesellschaft steigern zu können.

Finnland ist bei der Medienkompetenz seit vielen Jahren Spitzenreiter. Der nationalen Medienpolitik von 2019 zufolge wird Medienkompetenz derzeit als wichtiges Element der Bürgerkompetenz angesehen, die Menschen und Gemeinschaften breitere Möglichkeiten für ein gutes, sinnerfülltes Leben eröffnet. Sie ist fester Bestandteil nationaler Strategien und Lehrpläne und wird sowohl mit öffentlichen als auch mit privaten Geldmitteln gefördert. Dieses Thema ist auch oft Gegenstand des öffentlichen Diskurses, und da Redefreiheit sowie Vertrauen in die Medien für die Menschen in Finnland einen hohen Stellenwert einnehmen, erfahren Initiativen für Medienbildung breite Unterstützung. Bei

Finnlands multidisziplinärem, sektorübergreifendem und kollaborativem Medienkompetenzansatz arbeiten verschiedenste Stellen zusammen – Nichtregierungsorganisationen, Bildungseinrichtungen, Regierungsbehörden, Kommunen und AkteurInnen aus dem Privatsektor. Um hochwertige Bildungsprogramme zu erzielen, werden die Fachkräfte, die Medienkompetenz vermitteln sollen, umfassend geschult.

Durch Online-Umgebungen wandeln sich soziale, kulturelle, technologische und politische Aspekte unseres Lebens – sie können sich sogar auf den Verlauf von Konflikten und den Zustand von Demokratien auswirken und wurden als Triebfeder extremistischer Propaganda erkannt. Sich auf diesem Ozean aus Informationen zurechtzufinden, ist allermindestens herausfordernd, weshalb es unabdingbar ist, sich entsprechende Kompetenzen anzueignen und eine Resilienz gegenüber Falschinformationen aufzubauen. Dies ist uns nur möglich, indem wir voneinander lernen und Fachkenntnisse austauschen, auch über Grenzen hinweg.

***Veera Tuomala und Annukka Kurki** arbeiten für Save the Children Finland und sind auf P/CVE-Arbeit mit jungen Menschen sowie Radikalisierung im Internet spezialisiert. Im Abschnitt „PraktikerInnen des RAN“ erfahren Sie mehr über Veera und Annukka.*

Quellen:

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

<https://www.epc.eu/en/publications/In-chaos-they-thrive-The-resurgence-of-extremist-and-terrorist-group~32c800>

European Policies Initiative, Open Society Institute (2021). Indice 2021 d'éducation aux médias,

https://osis.bg/wp-content/uploads/2021/03/MediaLiteracyIndex2021_ENG.pdf

Mapping of media literacy practices and actions in EU-28, Observatoire européen de l'audiovisuel, 2016,

<https://rm.coe.int/1680783500>

Ministère de l'éducation et de la culture (2019). Éducation aux médias en Finlande : Politique nationale d'éducation aux médias,

<https://medialukutaitosuomessa.fi/mediaeducationpolicy.pdf>

Nordic Policy Centre (2020). Éducation aux médias en Finlande,

https://www.nordicpolicycentre.org.au/media_literacy_education_in_finlet

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

<https://www.epc.eu/en/publications/In-chaos-they-thrive-The-resurgence-of-extremist-and-terrorist-group~32c800>

Radicalisation Awareness Network



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.

Product of the Radicalisation Awareness Network
(RAN)



Radicalisation Awareness Network



CONCLUSION PAPER
 Digital grooming tactics on video gaming (adjacent) platforms
 Page 2 of 8

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.

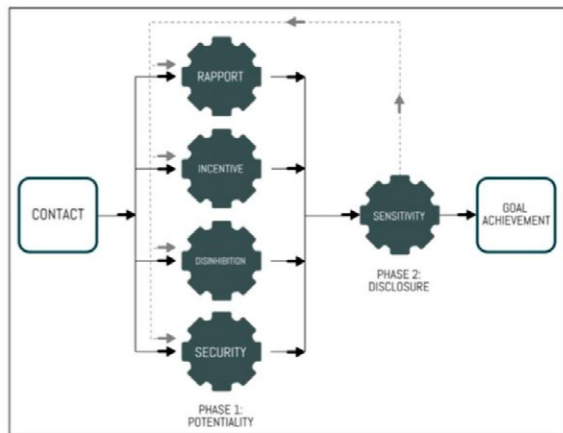



Figure 2. A self-regulation model of illicit grooming. Black solid lines/arrows indicate progress through the model; gray dashed lines/arrows indicate feedback loops.

Product of the Radicalisation Awareness Network
(RAN)



⁽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:
**An die Gamepads,
fertig, los: Gaming
und Extremismus
(prävention)**



**Linda
SCHLEGEL**

ÜBER die letzten beiden Jahre hat die potenzielle Verflechtung von Gaming und Extremismus einiges an Aufmerksamkeit erfahren. ForscherInnen, PraktikerInnen, politische EntscheidungsträgerInnen und internationale Organisationen wie EU und UN stufen die Entwicklungen in dieser Thematik als besorgniserregend ein. Dennoch ist überraschend wenig darüber bekannt, wie und warum ExtremistInnen nicht nur Videospiele selbst, sondern auch Inhalte und Plattformen mit Gaming-Bezug wie Discord und Twitch für sich nutzen.

Die RAN-Arbeitsgruppe Communications & Narratives (RAN Practitioners 2020) hat sechs konkrete Ansätze identifiziert, die sowohl DschihadistInnen als auch gewaltbereite RechtsextremistInnen in diesem Zusammenhang verfolgen:

- Die Produktion spezieller Computerspiele wie Special Forces von der Hisbollah oder Heimatdefender:Rebellion von der Identitären Bewegung
- Die Modifikation bestehender Computerspiele, etwa durch Nachstellung des Anschlags von Christchurch in Die Sims und Minecraft sowie die „Gründung“ eines weißen Ethnostaats auf der Plattform Roblox
- Die Nutzung der Chatfunktion in beliebten Onlinespielen, um mit (jungen) SpielerInnen zu kommunizieren und sie potenziell anzuwerben
- Der Missbrauch von Gaming-Plattformen wie Steam, Discord, Twitch oder DLive nicht nur zur internen Kommunikation und zu Anwerbungszwecken, sondern auch zur Planung oder gar Live-Übertragung von Gewalttaten, wie etwa beim Anschlag von Halle oder dem Sturm auf das US-Kapitol am 6. Januar 2021 (RAN Practitioners 2021a)
- Das Aufgreifen von Gaming-Kultur, etwa durch Nachbilden des visuellen Stils von Shootern in Propagandavideos oder explizite Anspielungen auf beliebte Videospiele wie Call of Duty
- Gamification – die Übertragung von Konzepten des Spieledesigns auf andere Kontexte – in ihrer Kommunikation, etwa in Form des Abschnitts

Obwohl in jüngster Zeit verstärkt daran gearbeitet wurde, die Nutzung von Gaming-Elementen und Gaming-bezogener Räume durch ExtremistInnen besser zu durchschauen, klafft nach wie vor eine breite Wissenslücke. Praktisch alles, was bis heute über die potenzielle Verflechtung von Gaming und Extremismus bekannt ist, basiert auf anekdotischer Evidenz und theoretischen Überlegungen. Weder kennen wir das Ausmaß des Problems, z. B. wie weit verbreitet extremistische Inhalte in der Welt der Spiele sind, noch wissen wir, ob ExtremistInnen Inhalte und Räume

mit Gaming-Bezug noch aus weiteren Gründen für sich nutzen möchten, als aufgrund ihrer Beliebtheit bei der potenziellen Zielgruppe und den Möglichkeiten, in privaten Gruppen der Moderation von Inhalten zu entgehen. Außerdem ist unklar, welchen Einfluss Gaming auf Radikalisierungsprozesse haben könnte – und ob überhaupt einer feststellbar ist. Trotz der Fortschritte der letzten Jahre stochert die P/CVE-Arbeit bei den wichtigsten Fragen zu Gaming und Extremismus nach wie vor im Trüben.

Das kürzlich eingerichtete Extremism and Gaming Research Network (EGRN) soll hier Klarheit schaffen und dazu beitragen, die bestehende Wissenslücke durch systematische und evidenzbasierte Untersuchung aufzufüllen. Auch wenn diese Arbeit sehr wichtig ist und P/CVE-AkteurInnen auf lange Sicht ermöglichen wird, sicherer mit diesen neuen Entwicklungen umzugehen, kann die Präventions- und Interventionsarbeit nicht einfach ausgesetzt werden, bis diese (oft sehr langwierigen) Forschungen abgeschlossen sind. Wir wissen zwar nicht genau, in welchem Umfang und aus welchen Gründen ExtremistInnen in Räumen mit Gaming-Bezug agieren, aber wir wissen durchaus, dass sie dies grundsätzlich versuchen und dass Gaming damit für die P/CVE-Arbeit von Bedeutung ist.

Bis heute wurde Gaming nur in äußerst wenigen Projekten berücksichtigt. Zusätzlich zu theoretischen Empfehlungen dazu, wie Gaming in P/CVE-Interventionen eingegliedert werden könnte (modus | zad 2021), ist auch ein gewisses Maß an Mut und Bereitschaft für „Versuch und Irrtum“ nötig, um mit der P/CVE-Arbeit in die Gaming-Welt vorzustoßen. Anders ausgedrückt: Um nicht länger als nötig im Blindflug zu bleiben und günstige Gelegenheiten verstreichen zu lassen, Gaming in Präventionsansätze einzubauen, während ExtremistInnen selbst in diesem Bereich aktiv sind, müssen P/CVE-AkteurInnen sich jetzt an Gaming-Inhalte heranwagen. Ohne die praktischen Erkenntnisse, die sich in solchen Projekten sammeln lassen, bleibt die Diskussion größtenteils abstrakt. Die sechs Wege, auf denen ExtremistInnen Spiele und Gaming-Plattformen für sich zu nutzen versuchen, könnten als Ausgangspunkt zur

Eingliederung von Gaming in die P/CVE-Arbeit dienen: Jede der sechs Komponenten der Typologie könnte auf die gleiche Weise, in der sie offenbar zur Radikalisierung genutzt wird, auch bei der Extremismusprävention herangezogen werden.

Trotz der klaren Belege dafür, dass ExtremistInnen das Gaming-Ökosystem für sich nutzen möchten, ist beim Entwurf von Projekten auf moralische Überheblichkeit zu verzichten, wie sie bei der Debatte um „Killerspiele“ und Amokläufe an Schulen ab den 1990ern zu beobachten war. Es gibt keine Belege, die darauf hinweisen, dass GamerInnen tendenziell anfälliger für Radikalisierung wären als beliebige andere Gruppen. Dennoch ist es als vielversprechend anzusehen, sich mit Gaming auseinanderzusetzen und entsprechende Erkenntnisse und Inhalte in die P/CVE-Arbeit zu integrieren – nicht nur, um ExtremistInnen in diesen Räumen entgegenzuwirken, sondern auch, um das enorme popkulturelle Potenzial auszuschöpfen, das Gaming innewohnt.

***Linda Schlegel** ist Doktorandin an der Johann-Wolfgang-Goethe-Universität Frankfurt, Research Fellow bei „modus | zad – Zentrum für angewandte Deradikalisierungsforschung“ sowie Associate Fellow bei der Hessischen Stiftung Friedens- und Konfliktforschung (HSFK). Ihre Forschung ist auf digitale Radikalisierung, Kampagnen für alternative und Gegen-Narrative, Storytelling sowie Gaming und Extremismus gerichtet.*

Quellen:

EGRN

[Link hier](#)

RAN Practitioners (2020), Nutzung von Videospiele durch ExtremistInnen – Strategien und Narrative

[Link hier](#)

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

[Link hier](#)

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

[Link hier](#)

INTERVIEW: Ein Tag im Leben von ... Viktoras Dauksas

SPOTLIGHT stellt dem Praktiker Viktoras Dauksas, der Bildungskampagnen für Medienkompetenz in baltischen Staaten, Osteuropa und dem Westbalkan durchführt, zehn Fragen zum typischen Arbeitstag bei „DebunkEU.org“.



**Viktoras
DAUKSAS**

Was macht DebunkEU.org?

DebunkEU.org ist eine unabhängige Technologie-Denkfabrik und Nichtregierungsorganisation, die Desinformation erforscht und Bildungskampagnen für Medienkompetenz durchführt. DebunkEU.org analysiert Desinformation in baltischen Staaten, Polen, Georgien und Montenegro und zusammen mit Partnerorganisationen auch in den USA und Nordmazedonien.

Aus welchem Anlass wurde die Organisation gegründet?

Die Annexion der Krim im Jahr 2014 war ein wichtiger Auslöser, der uns zur Desinformationsanalyse gebracht hat.

Was für Kampagnen führen Sie durch?

Im Kern unserer Arbeit stehen die Analyse von Desinformation, das Erstellen von Berichten und die Vermittlung der Erkenntnisse. Wir bieten aber auch Schulungen für Medienkompetenz an.

Eines der bedeutendsten Projekte im Jahr 2020 bestand darin, das Medienkompetenzspiel Bad News für Zielgruppen in Litauen, Lettland und Estland anzupassen – 118 000 Personen haben das Spiel ausprobiert. Anhand einer Befragung konnten wir feststellen, dass die Resilienz gegenüber Desinformation bei Personen, die das Spiel gespielt hatten, um 22,35 Prozent höher als bei der Kontrollgruppe lag.

Letztes Jahr begannen wir zusammen mit Hochschulen, unseren „Civic Resilience Course“ umzusetzen, und über 1000 Studierende testen ihn derzeit: <https://www.debunkeu.org/civic-resilience-course>

Welche Kampagnen erweisen sich als die erfolgreichsten, und warum?

Kurz- und mittelfristig betrachtet sind Desinformationsanalyse, Berichterstattung und die Vermittlung der Ergebnisse an Interessengruppen besonders wirksam. Langfristig sind Aus- und Weiterbildung am effizientesten.

Wie hat sich Ihre Arbeit seit der Coronakrise verändert?

Unsere Arbeitsauslastung hat sich vervierfacht. Zu Beginn der Pandemie war es schwierig, sich an die neuen Gegebenheiten anzupassen und Prozesse maßstäblich deutlich zu vergrößern. Dies nahm etwa fünf Monate in Anspruch.

Wie wirken sich die Ereignisse in der Ukraine und Belarus aus?

Die hybride Kriegsführung hat gewaltige Folgen für uns. Diese gewollte Krise zieht viel Aufmerksamkeit auf sich, und IT wird einem völlig neuen Maßstab aktiv eingesetzt.

Wie sieht ein typischer Arbeitstag bei DebunkEU.org aus?

Analyse, Analyse, Analyse!

Ein typischer Tag beginnt bei uns mit dem Morgenkaffee, bei dem wir unsere Mails checken und uns die Newsletter zu den neuesten Entwicklungen im Bereich Desinformation ansehen. Unsere Maxime lautet „Wahrheiten offenbaren sich erst, nachdem man vom köstlich duftenden Bohnennektar gekostet hat“, der Schluck Kaffee ist also fester Bestandteil unserer Vorbereitung auf ein Debunking.

Nach diesem Morgenritual kommen wir zum weniger bequemen Part, der den größten Teil unseres Alltags einnimmt: erhaltene Informationen prüfen und kodieren (oder „labeln“, wie wir es nennen). Dies ist eine komplexe und dynamische Tätigkeit, da unsere AnalystInnen den gesamten Inhalt daraufhin untersuchen, ob getroffene Aussagen faktisch richtig sind, mit welchen Techniken die LeserInnen überzeugt werden sollen und in welchem Kontext bestimmte Quellen, AutorInnen und Ereignisse stehen.

Nach Analyse des Inhalts tragen wir dann verschiedene Daten zum untersuchten Fall zusammen und interpretieren sie nach den in diesem Bereich angelegten Regeln und Praktiken. Anschließend wird der Bericht verfasst.

Wie wichtig ist das Team aus FaktencheckerInnen für Ihre Arbeit?

Das Feld der Desinformation ist ziemlich breit und wirkt sich auf das Leben der BürgerInnen aus. Je mehr Menschen und Organisationen in diesem Bereich arbeiten, desto besser, insbesondere in Bezug auf das Prüfen von Fakten und das Melden von Falschinformationen.

Was können wir 2022 von DebunkEU.org erwarten?

Wir reagieren weiterhin auf sich abzeichnende Entwicklungen und erweitern den Umfang, in dem wir Desinformation analysieren, um die Öffentlichkeit sowie Interessengruppen über Beeinflussungskampagnen auf der ganzen Welt auf dem Laufenden zu halten.

Außerdem werden wir unsere Arbeit in der Medienkompetenzbildung fortsetzen. Der erfolgreiche Start der Pilotversion unseres „Civic Resilience Course“ zeigt, dass eindeutig Bedarf für interaktive Lösungen besteht, um junge Menschen im Erkennen von Desinformation zu schulen. Daher arbeiten wir 2022 daran, den Kurs für noch mehr Länder zu lokalisieren und ihn Studierenden an verschiedenen Hochschulen anzubieten.

Wir führen auch unsere schulungsbasierten Projekte weiter. Für dieses Jahr haben wir uns die Gründung einer Debunk Academy vorgenommen, an der mehrere Programme angeboten werden, die sich an EinsteigerInnen sowie an Personen richten, die bereits im Bereich der Desinformationsanalyse tätig sind.

Wie können sich PraktikerInnen des RAN einbringen?

Wir stehen gemeinsamen Projekten offen gegenüber und wir laden auch PraktikerInnen zu unseren Schulungen, zu Praktika, zum Verfassen von Doktor- und Masterarbeiten und zu weiteren Projekten ein. Wir sind über unsere Website erreichbar: **DebunkEU.org**

IŠPŪSTI

MENKINTI

IŠJUOKTI

BAD NEWS

FEATURE

FALSIFIKU

ATRASTI

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

IŠKREIPTI

PRADĖTI ŽAISTI

Informacija ir kitos

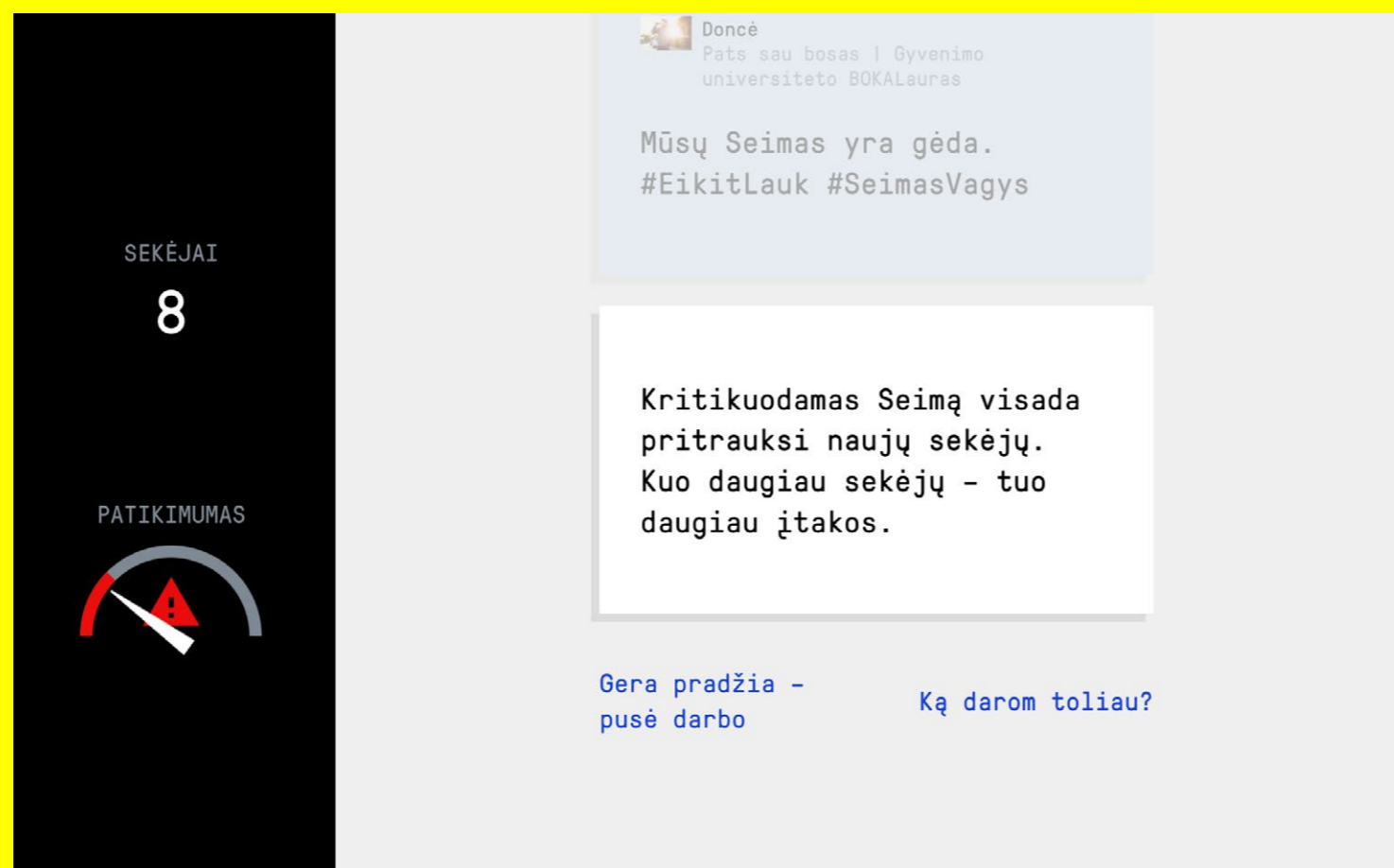
RĖKTI

INTRIGIOTI

PULTI

DAS SPIEL BAD NEWS

Von Mai bis Dezember 2020 führte DebunkEU ein Medienkompetenzprojekt in Litauen, Lettland und Estland durch, um die Resilienz der baltischen BürgerInnen mit einem Gamification-Ansatz zu steigern. Menschen in den baltischen Staaten (MuttersprachlerInnen der jeweiligen Amtssprache sowie des Russischen) wurden als Zielgruppe ausgewählt, da diese Region durchgehend mit falschen und irreführenden Informationen aus feindlich gesinnten Quellen bombardiert wird. Außerdem wird ein wesentlicher Anteil der in schlechter Absicht erstellten Inhalte auf Russisch verbreitet und zielt auf russische Minderheiten ab.



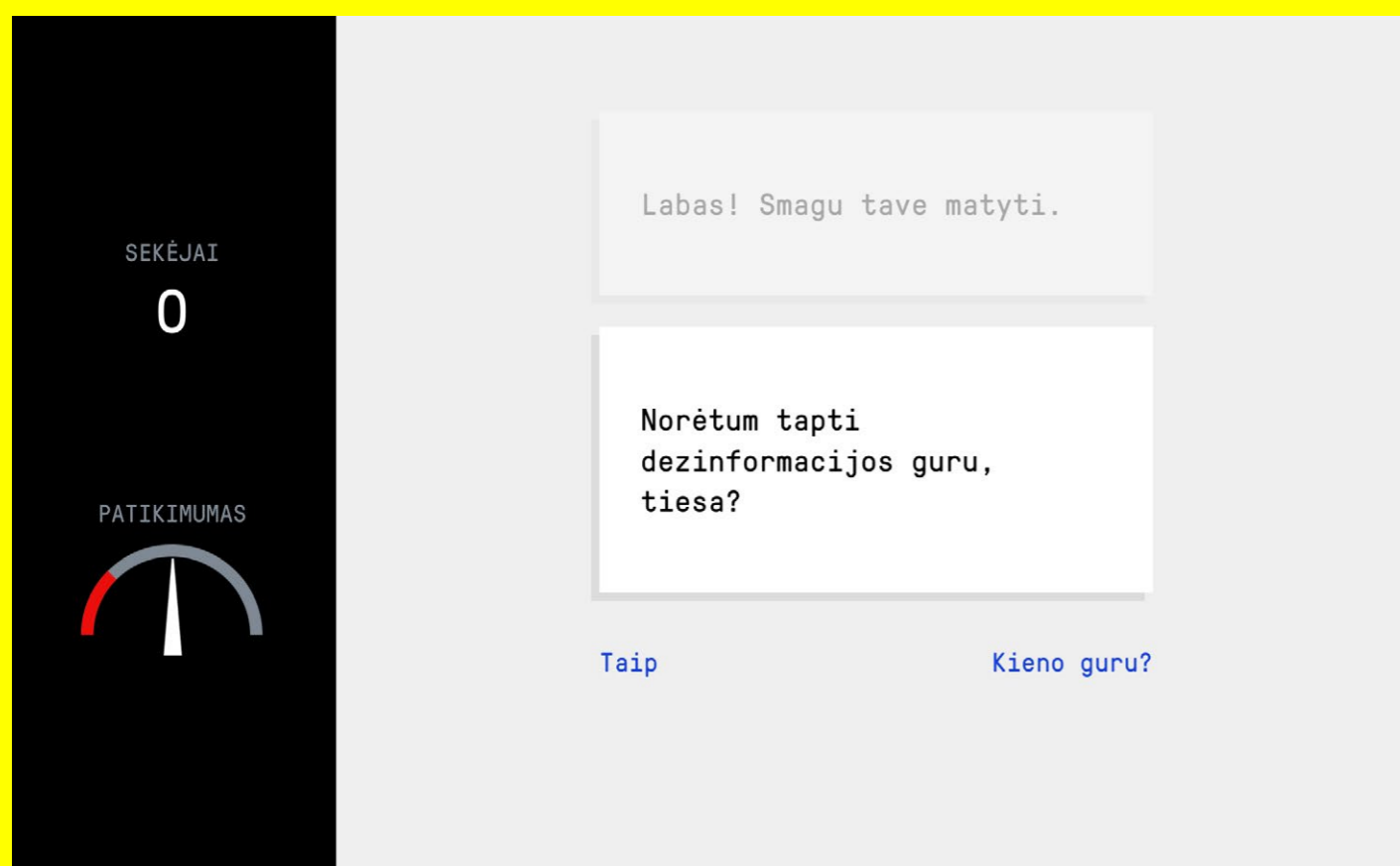
Daher wurde das vom niederländischen Medienkollektiv DROG und der Cambridge University entwickelte Spiel „Bad News“ als mögliche Lösung ausgewählt, um die Medienkompetenz in den baltischen Staaten zu steigern. Zuerst wurden es an ein Litauisch sprechendes Publikum in Litauen angepasst und später auch in Lettland und Estland präsentiert.

Insgesamt wurden sechs Seiten für Bad News erstellt – jeweils eine für die Zielgruppen in Litauen, Lettland und Estland sowie eine russische für jedes der drei Länder.

Bad News ist recht einfach aufgebaut und leicht verständlich: SpielerInnen sehen einen kurzen Text oder ein Bild (etwa ein Meme oder eine Schlagzeile) und können in unterschiedlicher Weise reagieren. Ihre Punktzahl misst sich in Followern und Glaubwürdigkeit. Wenn sie sich so verhalten, wie auch AkteurInnen in realen Desinformationskampagnen vorgehen würden, gewinnen sie an Followern und Glaubwürdigkeit. Wenn sie ihre Follower aber zu plump belügen, in ihrem Auftreten nicht ernst zu nehmen sind oder sich zu sehr an journalistische Standards halten, verlieren sie entweder Follower oder büßen an Glaubwürdigkeit ein. Ziel des Spiels ist, so viele Follower wie möglich anzusammeln, ohne zu viel Glaubwürdigkeit zu verlieren.

47 Fälle aus allen drei Ländern wurden ausgewählt und für das Spiel adaptiert, wobei die Wahl auf Meldungen fiel, die in den Zielgruppen viel Aufmerksamkeit erzeugt hatten. Die lokal ausgewählten Fälle ließen das Spiel realistischer wirken und zeigten, wie einfach im Internet falsche/irreführende Inhalte eingestellt werden können, wie sie verbreitet werden und mit welchen Techniken Zielgruppen beeinflusst werden.

Um den Erfolg des Projekts zu messen, führten wir zwei Befragungen durch: eine allgemeine und eine unter Personen, die Bad News gespielt hatten. Wir verglichen, wie sich die wahrgenommene Glaubwürdigkeit von Informationen im Internet veränderte, nachdem Menschen Bad News gespielt hatten, und stellten fest, dass die SpielerInnen die Informationen stärker



kritisch hinterfragten und ihnen weniger vertrauten als zuvor. Einer der größten Erfolge des Projekts bestand darin, dass die ältere Generation erreicht wurde. Gemäß den am Ende des Projekts gesammelten Daten zufolge lag der Anteil der SpielerInnen, die mindestens 55 Jahre alt waren, in Litauen bei 40 %, in Lettland bei 28 % und in Estland bei 35 %.

Außerdem stellten wir fest, dass die größte Wirkung bei jüngeren TeilnehmerInnen erzielt wurde – 35,5 % der BürgerInnen unter 34 in Litauen gaben an, dass sich ihre Resilienz erhöht habe, was gegenüber dem Durchschnitt von 22,35 % ein hervorragendes Ergebnis darstellt.

DebunkEU.org ist eine unabhängige Technologie-Denkfabrik und NRO, die Desinformation erforscht und Bildungskampagnen für Medienkompetenz durchführt. DebunkEU.org analysiert Desinformation in baltischen Staaten und Polen und zusammen mit Partnerorganisationen auch in den USA und Nordmazedonien.

Wenden Sie sich bei Rückfragen an:
Viktoras@DebunkEU.org

Weitere Beispiele für Projekte zum Thema Medienkompetenz finden Sie [hier](#) in der RAN-Sammlung inspirierender Praktiken.

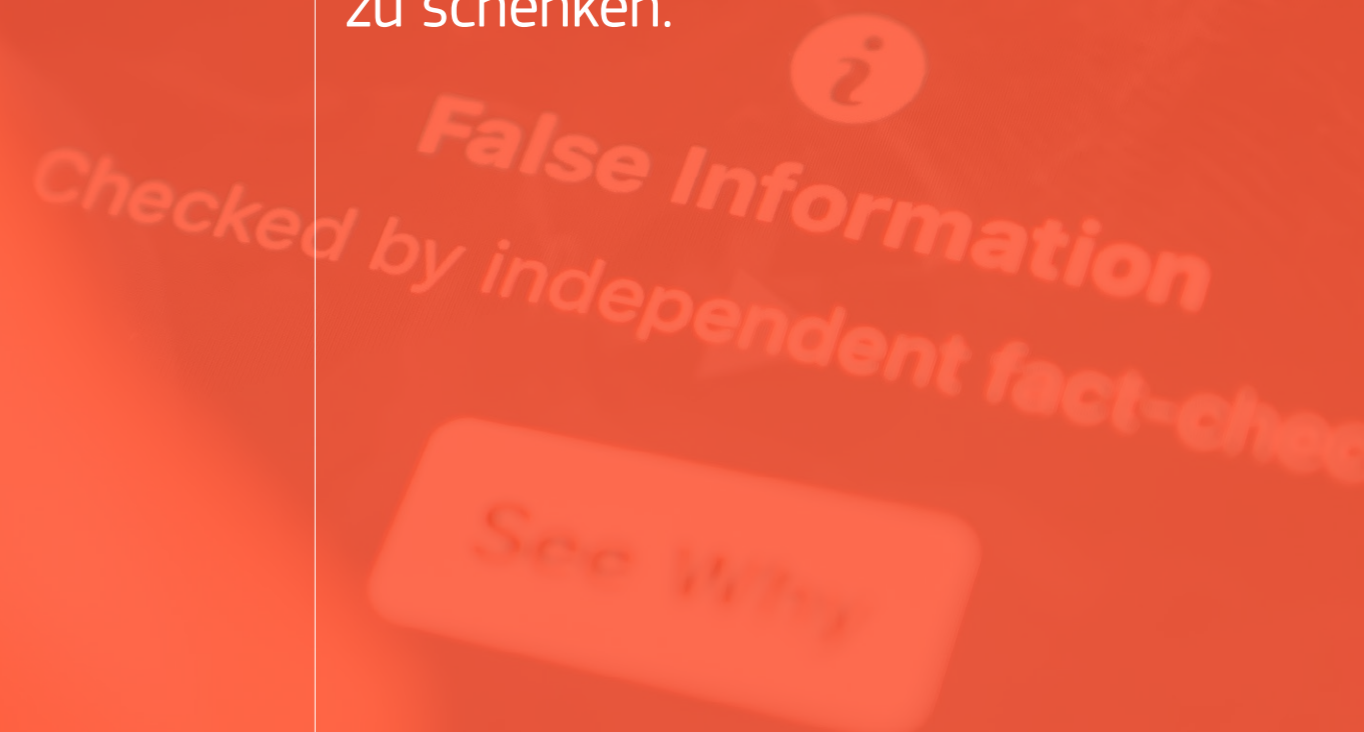
“Außerdem stellten wir fest, dass die größte Wirkung bei jüngeren TeilnehmerInnen erzielt wurde – 35,5 % der BürgerInnen unter 34 in Litauen gaben an, dass sich ihre Resilienz erhöht habe, was gegenüber dem Durchschnitt von 22,35 % ein hervorragendes Ergebnis darstellt.”

ARTIKEL:
**Die Inokulationstheorie
und ihre Anwendung
bei der Bekämpfung
von Desinformation**



**Rachel
FIELDEN**

Desinformation entwickelt sich stetig weiter und passt sich an, weshalb die Bemühungen zu ihrer Bekämpfung nachhaltig und ebenso anpassungsfähig sein müssen. Diese Herausforderung wird durch den Rabbit-Hole-Effekt noch verschärft, bei dem Personen, die zuvor Desinformation konsumiert und geglaubt haben, eher bereit sind, neuer Desinformation ebenfalls Glauben zu schenken.



Diejenigen von uns, die in diesem Bereich arbeiten, verfallen leicht in einen endlosen Kreislauf von Desinformation widerlegen und Fakten überprüfen, aber diese Methoden sind nur schwer in der Lage, die vielfältigen, komplexen und miteinander verknüpften Unwahrheiten, die gefährdete Personen glauben, zu erfassen. Dennoch ist die Widerlegung nach wie vor von großem Wert. Sie ist ein Kernelement des breiteren symbiotischen Ökosystems der Desinformationsbekämpfung, ähnlich wie Medienkompetenzschulungen oder das Zuordnen und Abziehen von MediatorInnen.

Nichtsdestotrotz müssen wir die Resilienz von Gruppen stärken, die anfällig für Desinformation sind und/oder sich bereits durch den Kaninchenbau der Desinformation bewegen. ForscherInnen haben sich dieser Herausforderung zum Teil durch das Studium des menschlichen Verhaltens und der Psychologie genähert, insbesondere durch die Entwicklung von Interventionsmethoden, die Menschen mit einer „psychologischen Resistenz“ gegen Desinformation ausstatten sollen, um sie aus einem Kreislauf des Glaubens zu befreien und ihnen eine langfristige Resilienz zu verleihen.

Diese Arbeit baut auf der Inokulationstheorie auf, die 1961 von William J. McGuire entwickelt wurde. McGuire fand heraus, dass Menschen dazu neigen, ihre Überzeugungen zu verteidigen, indem sie widerlegende Informationen meiden, anstatt aktiv nach Informationen zu suchen, die ihre Ansichten unterstützen.

Dieses Verhalten führt zu einem Mangel an Resilienz und kritischem Denken gegenüber Desinformation, insbesondere wenn diese Desinformation auf überzeugende Weise vermittelt wird und gut mit den bereits bestehenden Überzeugungen einer Person vereinbar ist.

Zwar kann diese Tendenz, widersprechende Beweise zu meiden, und die daraus resultierende kognitive Dissonanz eine anfällige Person in einen Kaninchenbau der Desinformation führen, sie kann aber auch dazu genutzt werden, psychologischen Widerstand gegen Desinformation aufzubauen. Mit anderen Worten: Unsere Denkprozesse können vor Beeinflussung oder Gegennarrativen geschützt werden, indem wir uns Desinformationstaktiken aussetzen.

In der Praxis lässt sich die Inokulation grob in vier Phasen unterteilen.

Phase 1: Konfrontation

Das Subjekt wird mit einer „Bedrohung“ konfrontiert, etwa einer desinformativen Aussage, die direkt unvereinbar mit einer faktischen Überzeugung einer Person ist und daher eine Bedrohung für diese darstellt. Damit die Aussage zur Inokulation wirksam sein kann, muss der Person klar sein, dass die neue Information eine direkte Bedrohung für ihre Weltanschauung darstellt.

Beispiel: „Deine Kultur wird angegriffen“ (dies funktioniert am besten, wenn die Bedrohung eindeutig ist).

Phase 2: Widerlegendes Ausschließen

Diese Phase wird aktiviert, wenn eine Person neue Informationen erhält, die nicht mit ihrer Weltanschauung übereinstimmen, wie im oben genannten Beispiel. Diese Botschaft wird dann mit einer Widerlegung gepaart, die die Schwächen des Arguments aufzeigt oder Gegenargumente liefert.

Beispiel: Argumente, die die Anschauung widerlegen, dass die eigene Kultur angegriffen werde. In diesem Prozess wird die Person einer schwachen „Dosis“ des „Virus“ ausgesetzt, für die Bedrohung durch Desinformation sensibilisiert und befähigt, die tatsächliche „Bedrohung“ in Zukunft besser zu erkennen und auf sie zu reagieren.

Phase 3: Verzögerung

Dies ist der Zeitraum zwischen der Inokulation und der Konfrontation mit der „tatsächlichen Bedrohung“, der erforderlich ist, um die schwache Version zu verarbeiten.

Phase 4: Involvierung

Das Subjekt ist in seinem Alltag einer tatsächlichen Bedrohung ausgesetzt (in diesem Fall extremistischer Desinformation über Einwanderer).

Die Forschung deutet darauf hin, dass die Inokulation nur dann funktioniert, wenn sich die Person für das Thema interessiert, damit die Phase des widerlegenden Ausschließens erneut ausgelöst wird. Im Jahr 2018 untersuchten ForscherInnen der University of Cambridge, wie sie die Inokulationstheorie in Inhalte umsetzen

können, die online abrufbar sind und das Gefühl der persönlichen Involvierung in die jeweiligen Themen fördern können. Gemeinsam mit dem niederländischen Medienkollektiv DROG entwickelten sie ein digitales Spiel namens Bad News, bei dem die SpielerInnen in die Rolle von PropagandaproduzentInnen schlüpfen, um Desinformation in der realen Welt anschließend besser zu erkennen.

Spiele sind eine sinnvolle Methode, um den passiven Konsum in eine aktive Auseinandersetzung mit einer Geschichte oder einem Thema umzuwandeln, was letztlich zu einer stärkeren persönlichen Involvierung der SpielerInnen führt. Es wurde festgestellt, dass der spielerische Inokulationsinhalt der Universität die Anfälligkeit für Fake-News-Schlagzeilen um durchschnittlich 21 % verringert. Ähnliche Projekte sind Harmony Square und Go Viral! – zwei großartige Beispiele dafür, wie die Inokulationstheorie in ansprechenden Online-Formaten eingesetzt wurde.

Bei Moonshot haben mein Team und ich unser eigenes Spiel entwickelt: Gali Fakta. Es kombiniert „Choose your own adventure“-Elemente mit einem realistischen Familien-Chat-Szenario. Ähnlich wie im richtigen Leben werden die SpielerInnen von ihrer „Familie“ einer Reihe von Unwahrheiten und anderen Desinformationstaktiken ausgesetzt. Entweder gelingt es ihnen, Fakten von Meinungen und Desinformation von Wahrheit zu unterscheiden, oder sie werden von ihrem Cousin entschieden, aber höflich zurechtgewiesen.

Bei einer Pilotstudie des Spiels im Jahr 2020 stellten wir fest, dass sich die SpielerInnen 12-mal so lange mit unseren Inokulationsinhalten beschäftigten, wenn diese in den Kontext eines Spiels eingebunden waren, als wenn dieselben Inhalte auf einer Website angezeigt wurden. 2021 haben wir eine Langzeitstudie über die Auswirkungen des Spiels auf die Verhaltensänderung in Bezug auf den Konsum von Desinformation begonnen. Und 2022 hoffen wir, das Spiel einem breiteren Publikum zugänglich machen zu können.

Die Arbeit von Moonshot und anderen PraktikerInnen aus der Branche ist Teil der wachsenden Bemühungen, die psychologische Resilienz gegenüber Desinformation zu stärken und gleichzeitig zu einer Evidenzbasis beizutragen, um die globalen Bemühungen zur Desinformationsbekämpfung zu unterstützen.

Rachel Fielden ist Analystin bei Moonshot und leitet deren Arbeit in Indonesien.

“Bei einer Pilotstudie des Spiels im Jahr 2020 stellten wir fest, dass sich die SpielerInnen 12-mal so lange mit unseren Inokulationsinhalten beschäftigten, wenn diese in den Kontext eines Spiels eingebunden waren, als wenn dieselben Inhalte auf einer Website angezeigt wurden. 2021 haben wir eine Langzeitstudie über die Auswirkungen des Spiels auf die Verhaltensänderung in Bezug auf den Konsum von Desinformation begonnen. Und 2022 hoffen wir, das Spiel einem breiteren Publikum zugänglich machen zu können.”

ARTIKEL: Die Überschneidungen zwischen terroristischen Online-Inhalten, Desinformation und der Reaktion des Technologiesektors



Anne
CRAANEN
and
Charley
GLEESON

Die terroristische Nutzung des Internets ist eine komplexe und vielschichtige Bedrohung, die eine ebenso nuancierte Reaktion erfordert. TerroristInnen nutzen ein breites Ökosystem aus Technologieplattformen für eine Vielzahl von Zwecken, die sich aus externer (öffentliche Propagandaverbreitung) und interner (operative Verwaltung) Kommunikation zusammensetzen. Unsere Analyse zeigt, dass innerhalb des Ökosystems der Technologieplattformen ein breites Spektrum von Klein- und Kleinstplattformen ins Visier genommen wird, die von Dienstleistern für File-Sharing, Video-Hosting und Bilder-Sharing bis hin zu Websites für Archivierung, Messaging und Copy-Pasting reichen. Tech Against Terrorism ist der Ansicht, dass dies ein Problem darstellt, da kleine Technologieunternehmen nicht über die Kapazitäten oder Fähigkeiten verfügen, um mit terroristischen Angriffen umzugehen. Daher unterstützen wir den globalen Technologiesektor dabei, der Nutzung ihrer Dienste durch gewaltbereite ExtremistInnen und TerroristInnen zu unterbinden und gleichzeitig die Menschenrechte zu wahren.

“Tech Against Terrorism ist der Ansicht, dass bei der Bekämpfung der terroristischen Nutzung des Internets ein unilateraler Ansatz verfolgt werden sollte, um alle potenziellen Möglichkeiten der terroristischen Instrumentalisierung zu analysieren und wirksame Gegenmaßnahmen ergreifen zu können. Die Bekämpfung der terroristischen Nutzung des Internets sollte auf akteursübergreifender Zusammenarbeit beruhen, um die Beziehungen zwischen öffentlichen und privaten Einrichtungen zu stärken und um sicherzustellen, dass die Reaktionen verhältnismäßig und der Bedrohung angemessen sind.”

Indem ExtremistInnen eine Vielzahl von Plattformen nutzen, bleiben die von ihnen veröffentlichten Inhalte insgesamt länger online, da die Entfernungspraktiken sich zwischen den verschiedenen Plattformen stark unterscheiden. Große Technologieplattformen sind in der Lage, automatisierte Algorithmen für die Moderation von Inhalten zu entwickeln und zu pflegen, während kleinere Plattformen dies nicht leisten können. Mehrere große Plattformen geben an, dass über 90 % der entfernten Inhalte durch automatische Methoden erkannt, gemeldet und entfernt werden, bevor sie NutzerInnen angezeigt werden. Im Gegensatz dazu verlassen sich kleine und Kleinstplattformen fast ausschließlich auf manuelle, menschliche Moderation, bei der die Erkennung und Entfernung schädlicher Inhalte wesentlich zeitaufwändiger ist. Online-Tools wie Spiegelungsdienste werden auch zunehmend von terroristischen AkteurInnen genutzt, um Inhalte weiterzuverbreiten und ihre Langlebigkeit im Internet zu gewährleisten. Um der Bedrohung durch terroristische Online-Inhalte wirksam begegnen zu können, ist daher ein kooperativer Ansatz erforderlich.

Die Entwicklung terroristischer Online-Inhalte hat sich in den Bereich von Desinformation und Verschwörungstheorien verlagert, insbesondere bei gewaltbereiten RechtsextremistInnen. Da die Grenzen zwischen terroristischen Inhalten, Desinformation und Verschwörungstheorien immer unschärfer werden, bewegen sich die InhaltsmoderatorInnen in einer Grauzone, in der sie bestimmen müssen, welche Inhalte die Schwelle zur Illegalität überschreiten. Einige Studien haben gezeigt, dass verschwörerisches Denken im Extremismus weit verbreitet ist und dass Verschwörungstheorien eine funktionelle Rolle in gewaltbereiten extremistischen Gruppen spielen. Tech Against Terrorism hat festgestellt, dass Desinformation und Verschwörungstheorien rund um COVID-19 gewaltbereiten rechtsextremen Bewegungen als Anwerbeinstrumente dienen, was insbesondere anhand der zunehmenden Überschneidungen zwischen Online-Inhalten deutlich wird. In ähnlicher Weise haben einige islamistische Terrorgruppen Propaganda mit Botschaften gegen COVID-19-Impfungen veröffentlicht, in denen es heißt, das Virus sei ein Akt Gottes. Die Manipulation mittels Desinformation und Verschwörungstheorien, insbesondere im Zusammenhang mit COVID-19, durch terroristische Gruppen stellt eine höhere Bedrohungsstufe dar, da terroristische

Organisationen sie wahrscheinlich zur weiteren Anwerbung und Radikalisierung einsetzen. Trotz der Schwierigkeiten bei der Moderation von Online-Inhalten stehen Technologieunternehmen an vorderster Front, wenn es darum geht, die Nutzung des Internets durch TerroristInnen zu unterbinden, indem sie Inhalte moderieren und dabei sowohl automatisierte als auch manuelle Methoden einsetzen. Die von Tech Against Terrorism entwickelte Terrorist Content Analytics Plattform (TCAP) identifiziert und verifiziert terroristische Inhalte mittels einer Kombination aus manuellen und automatisierten Open-Source-Intelligence-Methoden (OSINT). Die TCAP meldet dann URLs mit terroristischen Inhalten an Tech-Plattformen und unterstützt so die InhaltsmoderatorInnen beim Erkennen terroristischer Inhalte. Die TCAP hat damit begonnen, die Lücke bei der Inhaltsmoderation auf zahlreichen Plattformen zu schließen, indem es die ModeratorInnen auf verifizierte terroristische Inhalte aufmerksam macht. Seit der Einführung im November 2020 hat die TCAP über 13 000 URLs mit terroristischen Inhalten an 68 Plattformen gemeldet. 93 % dieser Inhalte wurden inzwischen entfernt.

Tech Against Terrorism ist der Ansicht, dass bei der Bekämpfung der terroristischen Nutzung des Internets ein unilateraler Ansatz verfolgt werden sollte, um alle potenziellen Möglichkeiten der terroristischen Instrumentalisierung zu analysieren und wirksame Gegenmaßnahmen ergreifen zu können. Die Bekämpfung der terroristischen Nutzung des Internets sollte auf akteursübergreifender Zusammenarbeit beruhen, um die Beziehungen zwischen öffentlichen und privaten Einrichtungen zu stärken und um sicherzustellen, dass die Reaktionen verhältnismäßig und der Bedrohung angemessen sind. Darüber hinaus verankern wir alle unsere Praktiken in der Rechtsstaatlichkeit und sorgen für gründliche Überprüfungsprozesse durch unabhängige PrüferInnen, wie unser transparentes Konzept für die TCAP zeigt.

Zusammenfassend lässt sich sagen, dass die Bekämpfung der terroristischen Nutzung des Internets die Zusammenarbeit öffentlicher und privater Stellen erfordert, um sicherzustellen, dass terroristische Inhalte rasch aus Online-Räumen entfernt werden können und gleichzeitig die Rechtsstaatlichkeit und die Menschenrechte umfassend gewahrt werden.

Wenn Sie mehr über Tech Against Terrorism erfahren möchten, abonnieren Sie den wöchentlichen Newsletter auf der Website techagainstterrorism.org. Folgen Sie der Organisation auch auf Twitter unter @TechvsTerrorism und @TCAPAlerts. Für weitere Fragen zur Arbeit der Organisation wenden Sie sich bitte an contact@techagainstterrorism.org.

***Anne Craanen** ist Senior Research Analyst bei Tech Against Terrorism und erforscht islamistischen Terrorismus und gewaltbereiten Rechtsextremismus sowie Geschlechterrollen im Terrorismus. Sie leitet das Forschungsteam bei Tech Against Terrorism und konzentriert sich außerdem auf OSINT-Analysen und die terroristische Nutzung des Internets. Sie ist verantwortlich für die Terrorist Content Analytics Plattform (TCAP), eine von Tech Against Terrorism entwickelte Plattform, die Technologieunternehmen auf terroristische Inhalte aufmerksam macht, wenn diese auf deren Plattformen gefunden werden. Anne hat einen MSc in Terrorismusbekämpfung und organisierter Kriminalität vom UCL und einen MA in Konfliktstudien vom King's College London. Zuvor hat sie bei Dataminr, Artis International und dem International Centre for the Study of Radicalisation (ICSR) gearbeitet.*

***Charley Gleeson** ist ein TCAP-Analyst bei Tech Against Terrorism. Ihre Arbeit am TCAP konzentriert sich auf OSINT und Politikentwicklung. Charley hat einen Hintergrund in forensischer Linguistik, terroristischer Propaganda und der Überschneidung von Technologie und Recht. Charley ist außerdem als Teamleiterin des Counter Threat Strategic Communications (CTSC)-Teams bei der Counterterrorism Group tätig und hat kürzlich einen Masterabschluss in Terrorismus- und Terrorismusbekämpfungsstudien an der Royal Holloway University of London erworben.*



Lone Actors in Digital Environments

Authored by Cathrine Thorleifsson
and Joey Düker, RAN External Experts

Radicalisation Awareness Network
RAN
Practitioners

LONE ACTORS IN DIGITAL ENVIRONMENTS

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 2011²⁴. 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 processes²⁶. A growing body of literature on political communication has highlighted the importance of social media platforms in spreading the views of RWE actors²⁷. Tech-savvy extremists from a new generation born into the digital age are utilising multiple platforms to forge communities and find social support to conduct acts of violence, including terrorism²⁸.

2.1 Online Platforms

In recent years, violent right-wing extremism has increasingly been characterised by young men who radicalise in transnational digital subcultures²⁹ 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 material³¹. This made it attractive for a loose network of channels known as "Terrorgram" that distribute content glorifying RWE lone actors³².

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-Aktivitäten zu EinzeltäterInnen

Wenn Sie teilnehmen, sich einbringen oder einfach mehr über die Arbeit von RAN Practitioners zum Thema EinzeltäterInnen erfahren möchten, finden Sie unten weitere Informationen.

Wegen der Corona-Pandemie werden die geplanten Aktivitäten online stattfinden. Die auf diesen Treffen gewonnenen Erkenntnisse und erzielten Ergebnisse werden im RAN Practitioners Update und auf der RAN-Website veröffentlicht. Zudem erfahren Sie Neuigkeiten auf den Social-Media-Kanälen des RAN.

Weitere Informationen über die Aktivitäten von RAN Practitioners finden Sie [hier](#) im Kalender auf der RAN-Website.



RAN-Arbeitsgruppe

Arbeitsgruppentreffen
Hybrid social work and digital awareness for families.



RAN-Arbeitsgruppe

Arbeitsgruppentreffen
Mind the gap: How to bridge the gap between the online and offline world.



RAN-Arbeitsgruppe

Arbeitsgruppentreffen
Exploring digital/hybrid exit and rehab work.



Webinar

Gamification of extremism.



Übergreifende Veranstaltung

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

LITERATURVERZEICHNIS

Erfahren Sie mehr

Wenn Sie mehr über die in diesem Magazin vorgestellten Themen und mit ihnen verbundene Lösungsansätze erfahren möchten, können Sie Kontakt zu den MitarbeiterInnen von RAN Practitioners aufnehmen, sich [die RAN-Sammlung inspirierender Praktiken](#) ansehen oder einige der neuesten [RAN-Beiträge lesen](#). Wir haben einige dieser Beiträge in die folgende sorgfältig ausgewählte Sammlung interessanter und relevanter Artikel aufgenommen.

RAN Practitioners (2021)
[Auswirkungen des digitalen
extremistischen Erbes auf die
Rehabilitation](#)

RAN Practitioners (2021)
[Digitaler Terrorismus und EinzeltäterInnen](#)

RAN Practitioners (2020)
[Der Wesenskern digitaler P/CVE-
Jugendarbeit: Tipps für praktisch Tätige](#)



European
Commission

Diese Veröffentlichung wurde von der Europäischen Kommission in Auftrag gegeben und von REOC Communications im Auftrag von RadarEurope, einer Tochtergesellschaft der RadarGroup, erstellt.