

UGent Impact Lab for Preventing and Countering Violent Extremism (P/CVE)

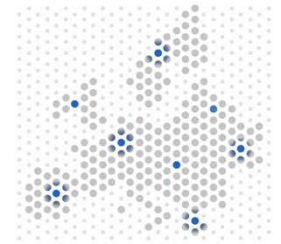
Prof. Dr. Wim Hardyns

Studiedag – Radicalisering en technologie: Veiligheidsperspectieven op fenomenen als extremisme en radicalisering, en de specifieke rol van technologie

24 oktober 2024



- Professor in de Criminologische Wetenschappen (UGent) en Veiligheidswetenschappen (UAntwerpen)
- ERC grant holder BIGDATPOL
- <https://www.linkedin.com/in/wim-hardyns-7250a129/>

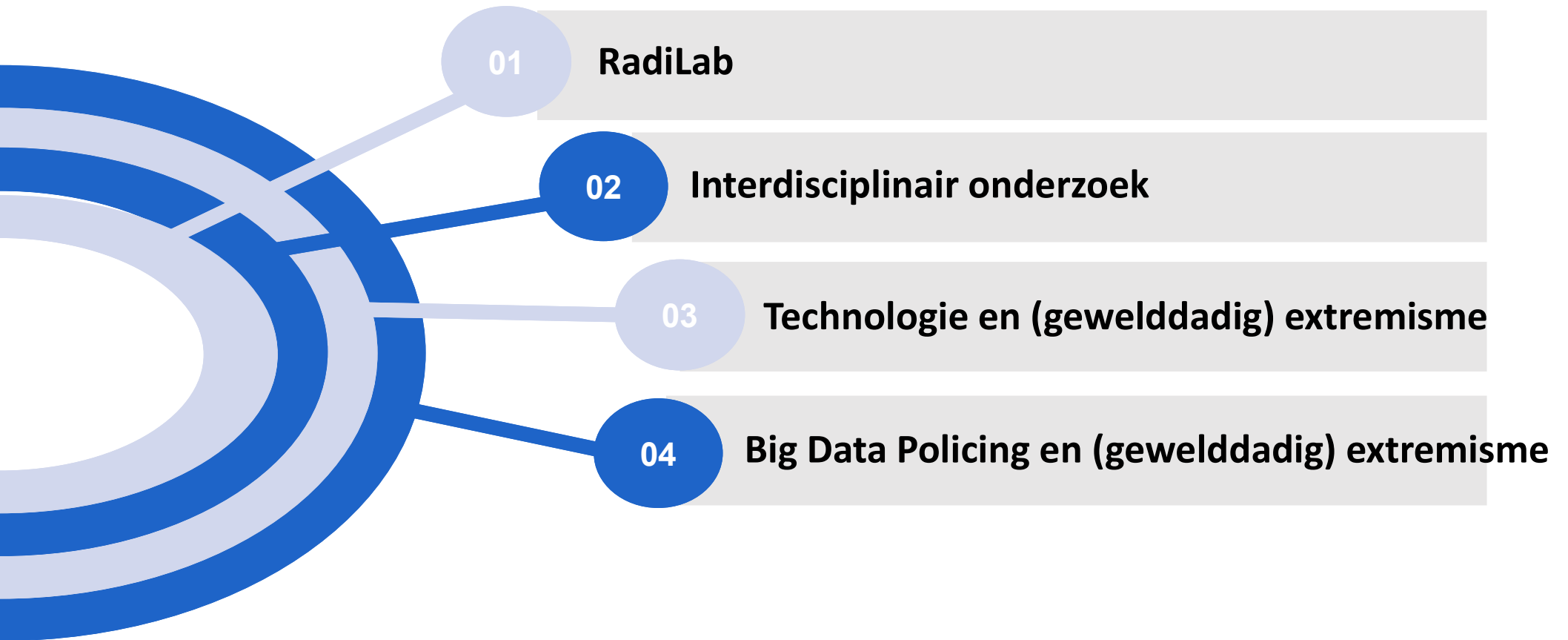


BIGDATPOL

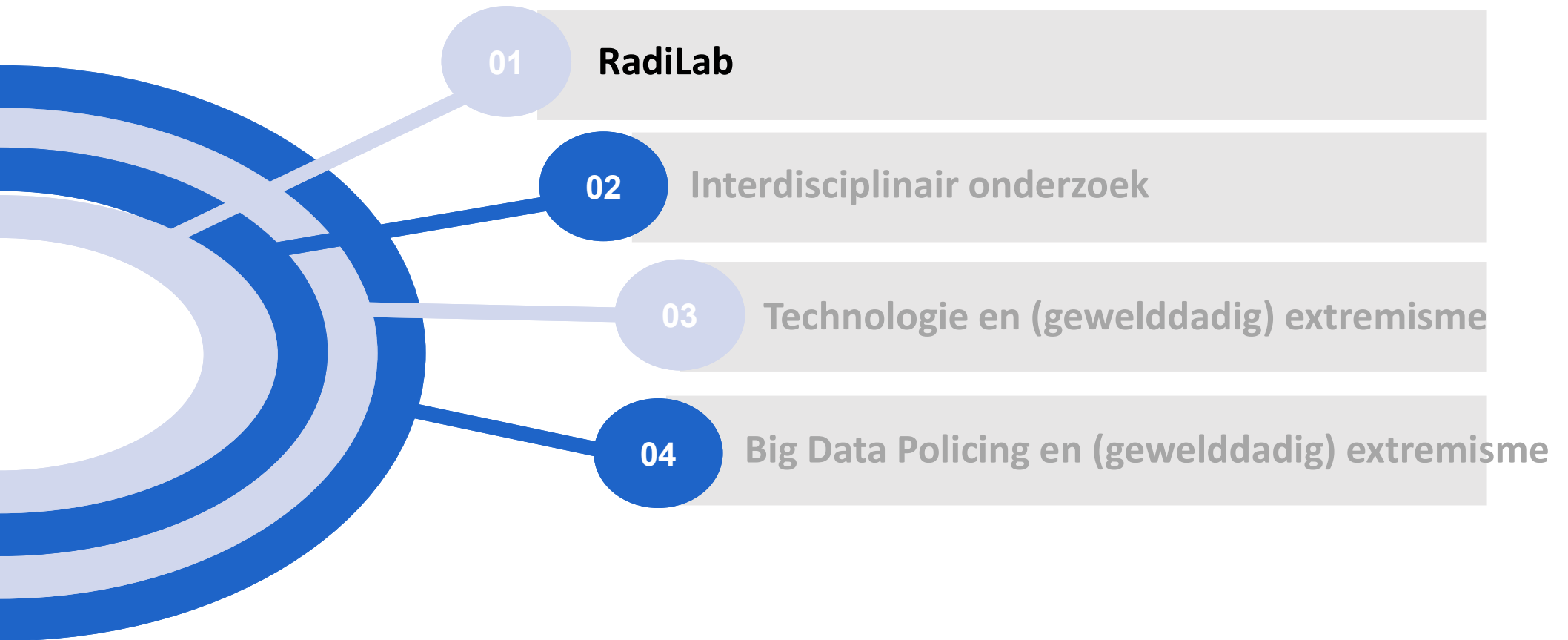
Towards an evidence-based
model for big data policing



INHOUDSTAFEL



INHOUDSTAFEL



1. RADILAB

Wie zijn we?

➤ Impact Lab → voorkomen en bestrijden van gewelddadig extremisme

➤ Samenwerking tussen:



➤ Interdisciplinair team: criminologen, juristen, psychologen, sociale wetenschappers, STEM, ...

➤ Partners: academici, openbare diensten, particuliere organisaties, maatschappelijk middenveld en beleidsmakers

→ lokaal, regionaal, (inter)nationaal

1. RADILAB

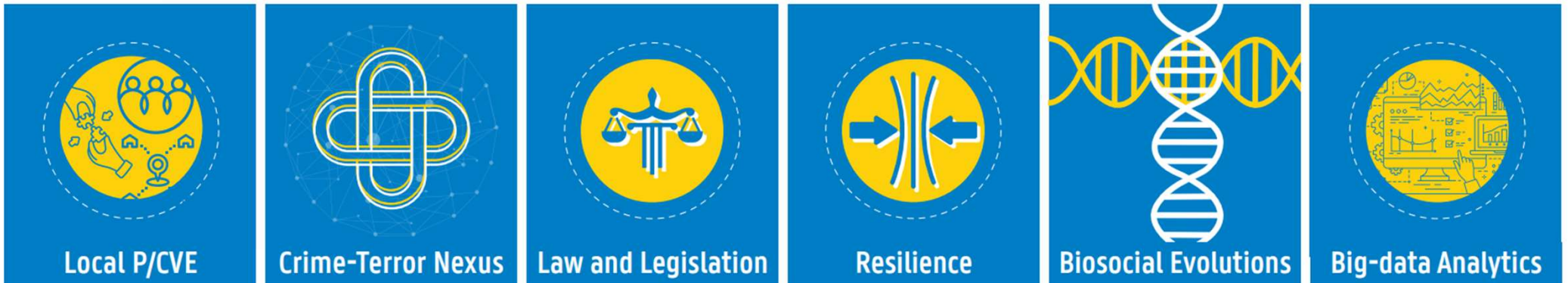
Wat zijn onze doelen?

- Bevorderen van inter- en transdisciplinaire samenwerking
- Samenbrengen van middelen en onderzoeksinfrastructuren
- Praktische implementatie van onderzoek en tools/instrumenten
- Creëren van impact
- Ondersteunen van onderzoekers/projecten adhv internationaal thematisch netwerk



1. RADILAB

Onze themagebieden



1. RADILAB

Wat doen we?

1. Wetenschappelijk onderzoek
2. Evaluatie van beleids-actieplannen
3. Ontwikkeling van tools en instrumenten
 - Kennis verspreiden naar praktijk + internationale kanalen

1. RADILAB

1. Wetenschappelijk onderzoek

01 October 2018 → 30 September 2023

One for all, all for one? A research into the steps toward violent extremism and terrorism: what it takes to make costly sacrifices.

Fellow: Lana De Pelecijn

Funding: Research Foundation - Flanders (FWO)



30 December 2021 → 29 May 2022

Desistance from Violent Extremism.

Fellow: Sigrid Raets

Funding: Regional and community funding: Special Research Fund

1. RADILAB

2. Evaluatie van beleids-actieplannen

VR 2021 2105 DOC.0553/3BIS

Actieplan ter preventie van gewelddadige radicalisering, extremisme, terrorisme en polarisatie

2020-2024

1. Inleiding

Het beleid ter preventie van gewelddadige radicalisering, extremisme, terrorisme en polarisatie werd uitgebouwd toen Vlaanderen werd geconfronteerd met jihadisme en vertrekkende Syriëstrijders (Foreign Terrorist Fighters of FTF). De gruwel van de terreurbewegingen Islamitische Staat en Al Qaeda was niet meer alleen iets uit het buitenland, maar nestelde zich ook in onze steden en gemeenten. Dit resulteerde in verschillende opvolgende aanslagen in het Westen, waaronder ook in ons land in 2016. Het feit dat bepaalde personen, voornamelijk jonge mannen, maar ook vrouwen en minderjarigen, binnen onze samenleving aangetrokken werden tot verschillende religieus-extremistische visies en daarin zelfs ook actie ondernamen, maakte een passende aanpak noodzakelijk.

Er werden de voorbije jaren al heel wat structuren, beleid en expertise uitgebouwd, zowel op federaal als op Vlaams niveau. Dit vertaalde zich in verschillende actieplannen: het Plan R op federaal niveau, en het Actieplan ter preventie van Gewelddadige Radicalisering en Polarisering op Vlaams niveau. Met een nieuwe Vlaamse regering, die nieuwe accenten legt en rekening houdt met enkele recente evoluties en ontwikkelingen, is er nood aan een herziening van het vorige Vlaamse actieplan.

De dreiging vanuit religieus-extremistische, meer bepaald salafistische en islamistische hoek blijft, als grootste dreiging voor terroristische aanslagen, aanwezig in onze samenleving. Daarnaast moeten we ook waakzaam zijn voor andere vormen van radicalisering en extremisme, want er zijn naast het religieuze ook rechts-extremistische en links-extremistische varianten. Zo is er ondertussen ook een opgang van rechts-extremistisch gedachtegoed merkbaar zowel in België als internationaal. Zowel de Staatsveiligheid als het OCAD stellen momenteel vast dat de bedreigingen en het extremistisch gedachtegoed in die zin geëvolueerd zijn. Ook Europol stelde in zijn Terrorism Situation and Trend Report (TE-SAT) 2020 dat gewelddadig rechts-extremisme in opmars is. Bij rechts-extremisme, waarbij bepaalde individuen zich vanuit racistische motieven of complottheorieën laten manipuleren door rechts-extremistische ideologieën, zijn er vooral nog – in vergelijking met een aantal andere Europese landen – een relatief beperkt aantal terreurdaden in ons land geweest. Maar als overheid moeten we preventief te werk gaan om ook die voedingsbodem aan te pakken. We hebben ook aandacht voor links-extremisme en voor rechts-extremistische stromingen en organisaties binnen de minderheidsgroepen in ons land. Want deze vorm van extremisme vormt een grote dreiging voor minderheden binnen die minderheidsgroepen. Alle reële dreigingen voor de democratie in ons land dienen dus aangepakt te worden, zowel bijvoorbeeld het Madkhalistisch Salafisme als Blood and Honour als de Grijeze Wolven.

1



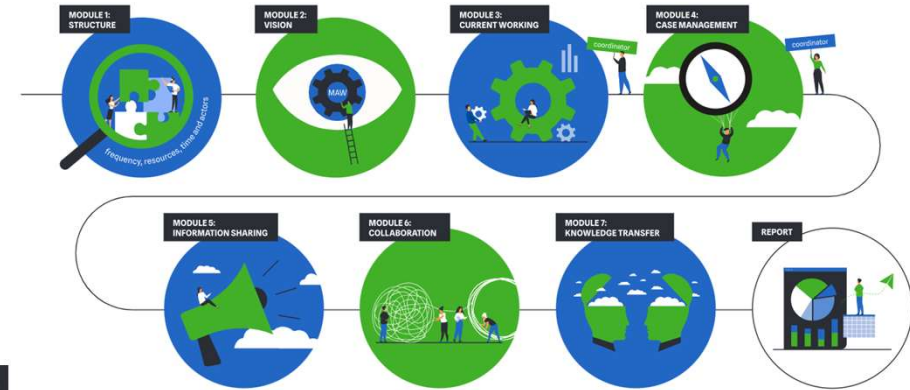
5

INHOUD

INHOUD	5
LIJST AFKORTINGEN	7
OVER DE AUTEURS	9
INLEIDING EN METHODOLOGISCHE VERANTWOORDDING Diederik Cops, Annelies Pauwels en Maarten Van Alstein	11
HOOFDSTUK 1 EEN TRANSVERSALE PROGRAMMACAN VAN HET VLAAMSE ACTIEPLAN TER PREVENTIE VAN GEWELDDADIGE RADICALISERING EN POLARISERING Wim Hardyns, Lieven Pauwels en Janne Thys	31
HOOFDSTUK 2 HET VLAAMSE ACTIEPLAN EN DE LOKALE AANPAK VAN GEWELDDADIGE RADICALISERING Lore Colaert en Maarten Van Alstein	89
HOOFDSTUK 3 ONDERWIJS EN DE PREVENTIE VAN GEWELDDADIGE RADICALISERING EN POLARISERING Kevin Goris	143
HOOFDSTUK 4 HET (HOO)WELIJNSWERK EN DE PREVENTIE VAN GEWELDDADIGE RADICALISERING EN POLARISERING Yamina Berrezeeg en Diederik Cops	207
HOOFDSTUK 5 ACTUELE UITDAGINGEN EN NODEN INZAKE GEWELDDADIGE RADICALISERING EN EXTREMISME Annelies Pauwels	259
HOOFDSTUK 6 HET VLAAMSE ACTIEPLAN GEËVALUEERD: ALGEMENE BESLUITEN Diederik Cops, Annelies Pauwels en Maarten Van Alstein	311

1. RADILAB

3. Ontwikkeling van tools en instrumenten



EMMASCAN

Home ForWhom? Manual Research → Start EMMASCAN → Coordinator English

Instructions for using the tool

The EMMASCAN provides multiple modules to evaluate the structure, vision, current working, case management, collaboration, information sharing and expertise of your local multi-agency working (MAW). The main goal of the self-evaluation tool is to allow a quick and easy evaluation of the Multi-Agency Working in your city/municipality. For more information about the indicators and the scoring process, please consult the EMMASCAN manual and the EMMA-project research report.

→ [Go to manual](#)

→ Start EMMASCAN



1. RADILAB

3. Ontwikkeling van tools en instrumenten

08 October 2018 → 02 October 2020

Developing and offering a programme for park guards and park animators with regard to the prevention of violent radicalisation

Funding: Regional and community funding: various



01 April 2018 → 31 December 2018

Development and animation of a training program for social assistants of the OCMWs for the prevention of violent radicalisms - pilot phase NL

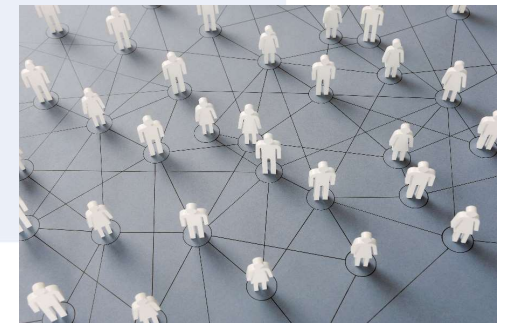
Funding: Regional and community funding: various



13 March 2020 → 13 March 2022

Developing and giving a training program 'Professional attitudes towards radicalisms and polarization' for social workers

Funding: Regional and community funding: various



1. RADILAB

3. Ontwikkeling van tools en instrumenten

06 December 2016 → 31 March 2019

BOUNCE- Reselience Training, Network and Evaluation - STRESAVIORA II

Funding: Federal funding: various

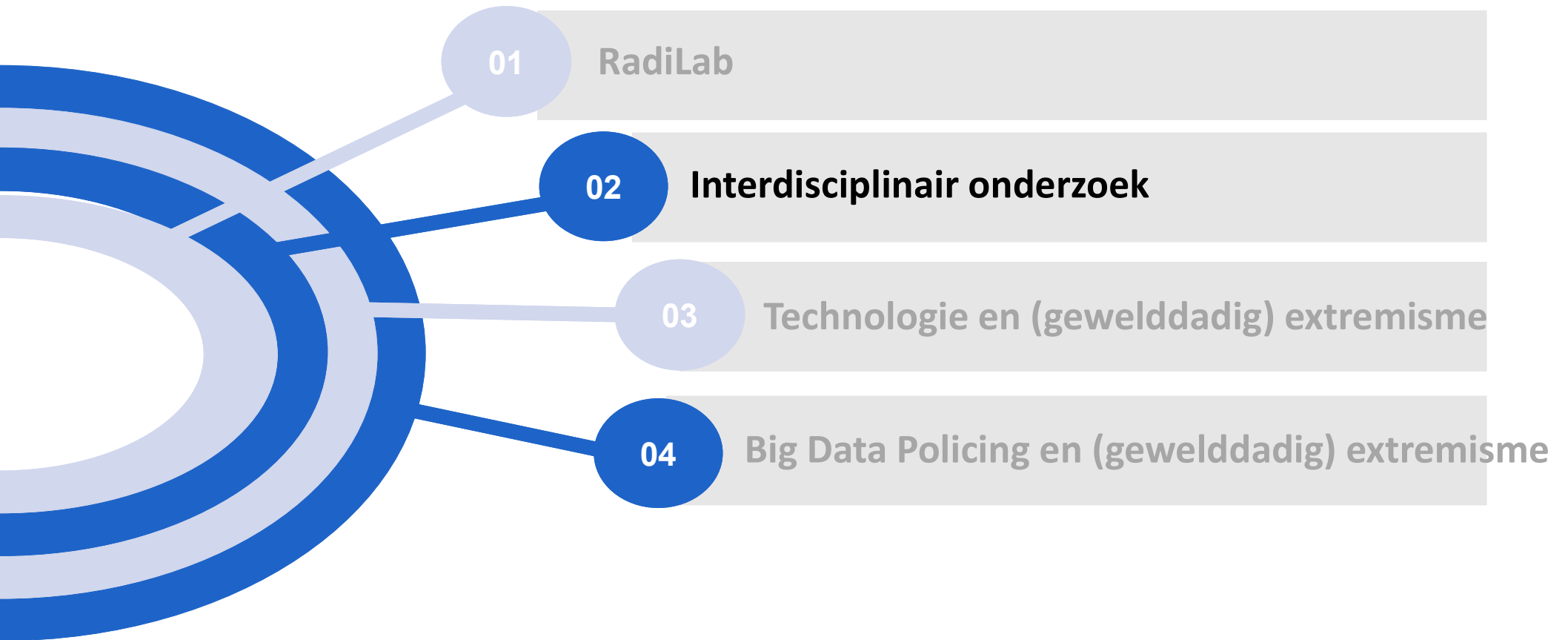
BOUNCE - VEERKRACHTTOOLS



BOUNCE versterkt de veerkracht en het kritisch denken van (kwetsbare) jongeren en maakt hun sociale omgeving bewust. BOUNCE heeft als doelstelling om de veerkracht van jongeren te verhogen, hun kritisch denken te stimuleren en de bewustwording bij ouders en eerstelijnsverleners te vergroten.



INHOUDSTAFEL



2. INTERDISCIPLINAIR ONDERZOEK



'Interdisciplinary research is a mode of research by teams or individuals that integrates information, data, techniques, tools, perspectives, concepts, and/or theories from two or more disciplines or bodies of specialized knowledge to advance fundamental understanding or to solve problems whose solutions are beyond the scope of a single discipline or field of research practice' (Giddens, 1991)

2. INTERDISCIPLINAIR ONDERZOEK

Criminologie

Sociologie

Politicologie

Taal-en
letterkunde

Computer
wetenschappen

Psychologie

Communicatie
wetenschappen

Rechten

Geschiedenis

Godsdienst
wetenschappen

Geografie

Pedagogische
wetenschappen

Bestuurskunde en
publiek
management

Economie

Filosofie

2. INTERDISCIPLINAIR ONDERZOEK

Politicologie

Prof. dr. em.
Rik Coolsaet

'Radicalisation' and 'Countering radicalisation': The emergence and expansion of a contentious concept

Rik Coolsaet

Hoofdstuk in een boek in **The Routledge Handbook on Radicalisation and Countering Radicalisation**

2024

(De)radicalisering tussen praktijk en ambiguïteit

Rik Coolsaet

A2 Artikel in een tijdschrift in **CAHIERS POLITIESTUDIES**
2017

When do individuals radicalize?

Rik Coolsaet

Hoofdstuk in een boek in **Contemporary terrorism studies**
2022

**Returnees : who are they, why are they (not) coming back and how should we deal with them ?
Assessing policies on returning foreign terrorist fighters in Belgium, Germany and the Netherlands**

Rik Coolsaet, Thomas Renard

Boek
2018

Rethinking radicalization : addressing the lack of a contextual perspective in the dominant narratives on radicalization

Rik Coolsaet, Stiene Ravn, Tom Sauer

Hoofdstuk in een boek in **Radicalisation : a marginal phenomenon or a mirror to society?**
2019

'All radicalisation is local': the genesis and drawbacks of an elusive concept

Rik Coolsaet

Boek
2016

Facing the fourth foreign fighters wave: what drives Europeans to Syria, and to IS? Insights from the Belgian case

Rik Coolsaet

Boek
2016

Deradicalisering en de IS generatie

Rik Coolsaet

Nieuwsartikel
2016

2. INTERDISCIPLINAIR ONDERZOEK

Taal-en
letterkunde

Prof. dr.
Catherine
Bouko

Online hate to offline harm : the impact of online hateful and extremist activity in our communities

Catherine Bouko
C3 Conferentie
2021

Discourse Patterns used by extremist Salafists in Facebook posts to potentially trigger cognitive biases

Catherine Bouko, Pieter Van Ostaeyen, Pierre Voué
C3 Conferentie
2021

Raising awareness about one's own cognitive biases to counter radicalization : presentation of the PRECOBIAS project

Catherine Bouko, Diana Rieger, Brigitte Naderer
C3 Conferentie
2021

Discourse patterns used by extremist Salafists on Facebook : identifying potential triggers to cognitive biases in radicalized content

Catherine Bouko, Brigitte Naderer, Diana Rieger, Pieter Van Ostaeyen, Pierre Voué
A1 Artikel in een tijdschrift in **CRITICAL DISCOURSE STUDIES**
2022

How jihadi Salafists sometimes breach, but mostly circumvent, Facebook's community standards in crisis, identity and solution frames

Catherine Bouko, Pieter Van Ostaeyen, Pierre Voué
A1 Artikel in een tijdschrift in **STUDIES IN CONFLICT & TERRORISM**
2024

Facebook's policies against extremism : ten years of struggle for more transparency

Catherine Bouko, Pieter Van Ostaeyen, Pierre Voué
A2 Artikel in een tijdschrift in **FIRST MONDAY (ONLINE)**
2021

Making students more resilient to extremist content online : critical thinking skills and self-awareness of cognitive biases

Catherine Bouko, Alena Krempaska, Anna Kucinska
Boek
2021

2. INTERDISCIPLINAIR ONDERZOEK

Economie

Prof. dr.
Ilse Ruysen

Leaving terrorism behind? The role of terrorist attacks in shaping migration intentions around the world

Killian Foubert, Ilse Ruysen

A1 Journal Article in **JOURNAL OF ETHNIC AND MIGRATION STUDIES**
2024

Prof. dr.
Stéphanie De
Coensel

Rechten

01 October 2016 → 30 September 2020

Legitimacy of a possible criminalisation of radicalism and/or extremism

Fellow: Stéphanie De Coensel

Funding: Regional and community funding: Special Research Fund

Psychologi
e

Prof. dr.
Alain Van Hiel

A radical vision of radicalism : political cynicism, not incrementally stronger partisan positions, explains political radicalization

Alain Van Hiel, Jasper Van Assche, Tessa Haesevoets, David De Cremer, Gordon Hodson

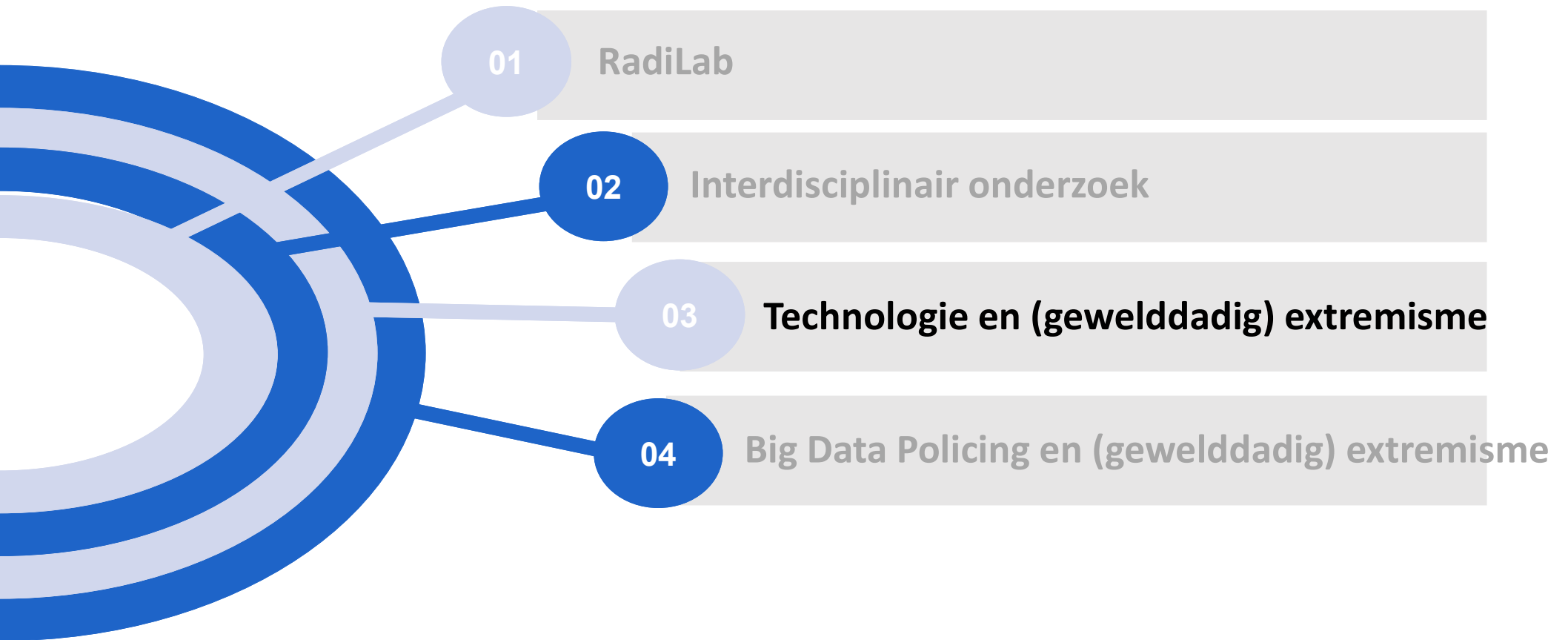
A1 Journal Article in **POLITICAL PSYCHOLOGY**
2022

...

Multimodale Detectie van Radicalisering



INHOUDSTAFEL



3. TECHNOLOGIE EN (GEWELDDADIG) EXTREMISME

ALS

FACILITATOR

VAN

EXTREMISME

TER

PREVENTIE/BESTRIJDIN

G

VAN EXTREMISME

3. TECHNOLOGIE EN (GEWELDDADIG) EXTREMISME

ALS

FACILITATOR

VAN

EXTREMISME

TER

PREVENTIE/BESTRIJDIN

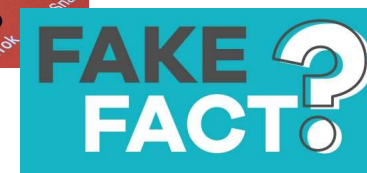
G

VAN EXTREMISME

3. TECHNOLOGIE ALS FACILITATOR VAN EXTREMISME

1. Gevoeligheid voor en verkenning van extremistische ideologieën

- Sociale media
- Fake news
- Chatbot
- ...

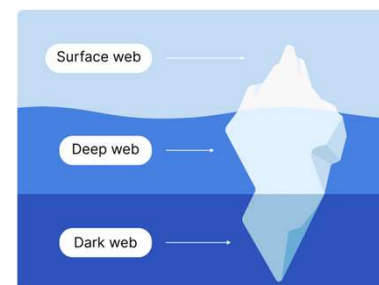


2. Lid van extremistische groep

- Communicatie
- Propaganda
- Deepfakes
- ...

3. Gewelddadig extremistische actie

- Dark web
- 3D-printer
- Cyberaanval
- ...



3. TECHNOLOGIE ALS FACILITATOR VAN EXTREM

Confronting Violent Extremism in Kenya
Debates, Ideas and Challenges

An Assessment of the Harms Associated With Ideologically Motivated Cyberattacks

Thomas J. Holt, Steven Chermak, [...] and Emily Greene-Colozzi [View all authors and affiliations](#)

OnlineFirst | <https://doi.org/10.1177/00111287241271221>

Understanding Online Radicalisation Using Data Science

Victoria Saggar, Charles Bart, University, Albany, Australia

ABSTRACT
What characterises social media radicals? And why some people become attracted to radicalisation? To explore answers to these questions, a number of tweets posted by a group of suspected radicals tweeting in Arabic were analysed using social network analysis and machine learning. The study revealed that these suspected radicals' networks showed significant interaction with others, but this interactivity is only significant quantitatively as the interaction is not reciprocal. With regards to why these suspected radicals became attracted to radicalisation, Topic Modelling revealed these suspected radicals' tweets underpinned a perceived injustice that they believed the Secret Police and the Government inflicted upon them. Overall, the study has shown that data science tools have the potential to inform our understanding of online radicalisation. It is hoped this exploratory study will be the basis for a future study in which the research questions will be answered using a larger sample.

KEYWORDS
Data Science, Extremism, Machine Learning, Radicalisation, Social Network Analysis

INTRODUCTION
The extremist who took part in gunning his soldier cousin in Saudi Arabia in 2015 was young as 18 years old and the gamer himself was only 21 years old. All of the four suicide bombers who carried out attacks on mosques during the Friday prayers in Saudi Arabia in 2015 aged between 20 and 23 years. The fact that these attackers were this young suggests that radical groups can easily infect young people with the 'radicalisation virus'. 'Radicalising' young people, who may not yet fully understand the grey areas surrounding right and wrong and who may not have the skill to easily and rationally analyse the outcomes of their actions, can have devastating consequences for people's safety worldwide.

Radicals live by the rule 'divide and conquer'. After dividing people into groups, they move to establishing their credibility to the groups they target (Al-Saggar, Hinson & Khanbush, 2009). Once this is achieved, they progress to communicating their ideology, explaining where they differ with others and providing the 'justification' for their thinking, which they often back up with 'evidence' (Al-Saggar & Khanbush, 2009). However, their attempts to advocate violence in Saudi online communities, i.e. before the widespread adoption of social media, achieved limited success, as evidenced by fewer and smaller suicide terrorist activities compared to the multiple, large attacks post the social media era.

One reason for this is because radicals were not alone in the Saudi online communities in which they operated (Al-Saggar & Khanbush, 2009). The results of one study showed that there were twice as many non-radicals in these online communities, which to some extent dented their voices.

5

Fathima Azmyia Badurdeen

Online Radicalisation and Recruitment: Al-Shabaab Luring Strategies with New Technology

Is AI-Generated Extremism Credible? Experimental Evidence from an Expert Survey

Stephane J. Baele, Elahe Naserian & Gabriel Katz

Published online: 02 Aug 2024

[Cite this article](#) | <https://doi.org/10.1080/09546553.2024.2380089> | [Check for updates](#)

Literature review

The impact of digital communications technology on radicalization and recruitment

ALEXANDER MELEGROU-HITCHENS, AUDREY ALEXANDER AND NICK KADERBHAH

Introduction
In 1997, David Duke, the figurehead of America's white supremacist movement, wrote that the internet would help to 'facilitate a worldwide revolution of White awareness' by circumventing the mainstream media. 'Years later, in 2000, global jihad strategist Abu Musab al-Barni argued that Al-Qaeda's 'informational resistance' against the West must be 'spearheaded through the use of modern technology of all forms, especially satellite and the Internet.' Worlds away from each other, Duke and Al-Barni shared a vision for their respective movements: if used effectively, contemporary media technologies were the key to success.

With the rise of right-wing and jihadist movements, the current security climate drives the demand for insights into the complex and evolving venues of violent extremism in the digital sphere. While it is undeniable that extremist groups across the ideological spectrum have identified digital communications technologies as an important resource, the precise impact of these mediums remains unclear. Consequently, this article presents a literature review to provide an up-to-date account of the role of digital communications in the process of radicalization and recruitment.

By surveying existing research, the review invites to interrogate three central questions: **Q1: How do digital communications technologies facilitate radicalization and recruitment?**

- Q2: What is the relationship between violent extremists and communication technologies?**
- Q3: How do digital communications technologies transformed radicalization and recruitment dynamics?**
- Q4: Can social dynamics in the digital sphere replace, or have a similar impact to, those in the physical world among extremist groups and their sympathizers?**

After providing clarification and context, the following sections will draw on works that investigate the relationship between media communication and violent radicalization and recruitment. First, this review will examine the connection between digital communications and recruitment.

© 2024, Elsevier B.V. All rights reserved. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

Global Network on Extremism & Technology

Encrypted Extremism Inside the English-Speaking Islamic State Ecosystem on Telegram

BENNETT CLIFFORD AND HELEN POWELL

Program on Extremism
THE ROYAL INSTITUTE FOR DEFENCE STUDIES

Offline Versus Online Radicalisation: Which is the Bigger Threat?

Tracing Outcomes of 439 Jihadist Terrorists Between 2014–2021 in 8 Western Countries

Nafees Hamid and Cristina Ariza

GNET is a special project delivered by the International Centre for the Study of Radicalisation, King's College London

MECHANISMS OF ONLINE RADICALISATION: HOW THE INTERNET AFFECTS THE RADICALISATION OF EXTREMIST-TIGHT LINE ACTOR TERRORISTS

Guri Nordtorp Malmer* and Jacob Aslaand Randalv

ABSTRACT
How does the internet affect the radicalisation of extreme-right line actor terrorists? In the absence of an established theoretical model, this article identifies six mechanisms with particular relevance for explaining online radicalisation. Having first reviewed a larger set of relevant line actor terrorists, the study track traced mechanisms in three selected cases where the internet was reportedly used intensively during radicalisation. The findings show that the internet primarily facilitated radicalisation through information provision, as well as amplifying group polarisation and legitimising extreme ideology and violence through echoing. In all three cases, radicalisation was also affected considerably by other push-factors that through their presence made extreme online messages more impactful. The results challenge the view that offline interaction is necessary for radicalisation to occur but also show that online influence itself is sufficient.

INTRODUCTION
The exponential development of the internet and social media has made it possible for extremists of all kinds to communicate and spread their ideas to a larger audience than before. The role played by the internet in fostering radicalisation has therefore become a pervasive subject in discussions of violent extremism among scholars and policymakers (Cortney, 2017, p. 77).

Existing research on the role(s) played by the internet in radicalisation is scarce, often descriptive, and neglects with research gaps. First, there is an abundance of research on the 'supply' side of online extremist content, rather than how interaction with this content impacts radicalisation. Meanwhile, the 'demand' side of online radicalisation, i.e. how individuals engage with the internet, remains underexplored (Blattberg et al., 2020; von Behr et al., 2013). Second, there seems to be an imbalance in existing research stemming from an enduring focus on Islamic extremism, while other forms of extremism such as the extreme right have received less attention (Feldman, 2018, p. 40; Wroster et al., 2018).

Printing Terror: An Empirical Overview of the Use of 3D-Printed Firearms by Right-Wing Extremists

By Yannick Veilleux-Lepage

The last decade has seen a rapid proliferation in the use of 3D-printed firearms by right-wing extremist actors, presenting significant new challenges for law enforcement in countering political violence. This article provides an empirical overview of right-wing extremist adoption of 3D-printed firearms (3DPF) from political violence around the world. It analyses the geographical and temporal spread of 3DPF use by RWE and outlines four main motivations: symbolic and ideological reasons, supplementing conventional firearms, using 3DPF as alternatives when legal acquisition is difficult, and financing other activities or profiting from sales. The study emphasises the need for continuous monitoring, enhanced forensic techniques, and international cooperation, in addition to adapting law enforcement strategies and developing policies to address the evolving threats posed by 3DPF. As such, it provides an empirical foundation for further research and policy development into extremist use of 3D-printed firearms.

Offline Versus Online Radicalisation: Which is the Bigger Threat?

Tracing Outcomes of 439 Jihadist Terrorists Between 2014–2021 in 8 Western Countries

Nafees Hamid and Cristina Ariza

GNET is a special project delivered by the International Centre for the Study of Radicalisation, King's College London



3. TECHNOLOGIE EN (GEWELDDADIG) EXTREMISME

ALS
FACILITATOR
VAN
EXTREMISME

TER
PREVENTIE/BESTRIJDIN
G
VAN EXTREMISME

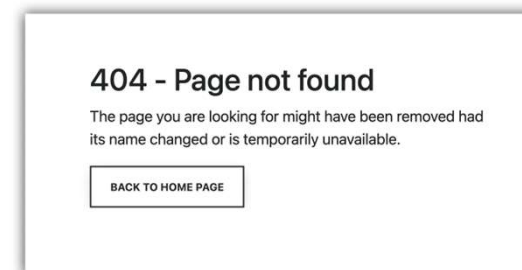
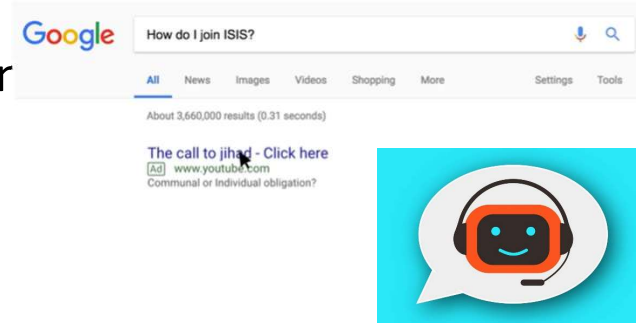
3. TECHNOLOGIE TER PREVENTIE EN BESTRIJDING VAN EXTREMISME

1. Gevoeligheid voor en verkenning van extremistische ideologieën

2. Lid van extremistische groep

3. Gewelddadig extremistische actie voorbereiden/uitvoeren

- Identificeren van vatbare personen
- chatbots, targeted ads, redirect methode
- Counter narrative
- ...
- Netwerkanalyses
- Content removal: extremistische accounts, haatspraak, beeldmateriaal
- ...
- Financiële transacties analyseren
- Cybersecurity
- ...



3. TECHNOLOGIE TER PREVENTIE EN BESTRIJDING VAN

Countering violent extremism using social media and preventing implementable strategies for Bangladesh

Sajiul Anis¹, Lambis Rana², Abdulla Al Kafy³

¹Center for Strategic Studies, Ministry of Education Bangladesh (CMSE), Dharam, Dhaka 1000, Bangladesh

²ICT for Social Justice, Center for Social Justice, Dhaka

³Department of Applied History, Faculty of Education, Dhaka University, Dhaka 1000, Bangladesh

ABSTRACT

Violence, from the 1970s to Bangladesh, has been prevented or mitigated through various social media through the internet and social media. This paper presents an overview of counter-terrorism (CT) work through the internet and social media. It discusses the current state of research on CT work through the internet and social media. It also discusses the current state of research on CT work through the internet and social media. It discusses the current state of research on CT work through the internet and social media.

1. Introduction

Violence, from the 1970s to Bangladesh, has been prevented or mitigated through various social media through the internet and social media. This paper presents an overview of counter-terrorism (CT) work through the internet and social media. It discusses the current state of research on CT work through the internet and social media. It discusses the current state of research on CT work through the internet and social media.

ME

Countering violent extremism on social media

An overview of recent literature and Government of Canada projects with guidance for practitioners, policy-makers, and researchers

Suzanne Waldman
Simona Verga
DRCDC - Centre for Security Studies

Defence Research and Development Canada
Scientific Report
DRDC-RDDC-2016-R229
November 2016

BRENNAN CENTER FOR JUSTICE

TWENTY YEARS

COUNTERING VIOLENT EXTREMISM

Faiza Patel and Meghan Koussik

Brennan Center for Justice at New York University School of Law

Countering Online Radicalisation during the COVID-19 Pandemic: The Case of Malaysia

Akil Yunus

Synopsis

The COVID-19 pandemic has strained the physical operations of terrorist networks but they have been able to adapt to an online radicalisation and recruitment activities. Countering violent extremist narratives and propaganda continue to spread widely on social media and have been effective around misinformation campaigns and conspiracy theories about the virus. Similarly, violent extremist groups have exploited the upsurge in online hate speech and xenophobia to further fuel communal tensions and attract new followers. Malaysia has recognised the need for multi-stakeholder approaches in tackling online radicalisation – involving not just state agencies but also civil society, youths and the media. One such idea is to develop digital resilience at the community level or more effectively counter online susceptibility to violent extremism.

Introduction

With the territorial defeat of the Islamic State (IS) and deceleration of its key operations by 2019, the group has become even more reliant on online messaging and recruitment activities to stay relevant. The group's ideology and propaganda continue to be popular on social media platforms and broader to procure a fresh generation of recruits and sympathisers. IS' survival is largely dependent on these remote foot soldiers, who self-radicalise online through engagement with propaganda resources and are then driven to plan and launch localized attacks. Recent terrorist incidents involving so-called lone wolf actors such as the New Zealand mosque attack and the bombing of a Hindu temple in France demonstrate the harmful consequences of online radicalisation. Greater balancing efforts to curb this trend, including investments in counter-messaging, internet and social internet regulations, terrorist activity in cyberspace is a more realistic response to internet and website compliance.

In recent years, governments have started exploring preventive strategies that not only address the immediate threat posed by terrorist activities, but also tackle the key drivers of violent radicalisation online and offline. Recognising that socio-economic vulnerabilities and communal grievances are among the factors that increase a nation's susceptibility to violent extremism (VE), multi-stakeholder or whole-of-society approaches have been touted as holistic solutions to achieve long-term outcomes, such as community resilience and social cohesion.¹

In the Malaysian context, these efforts have manifested in a number of ways. In 2021, the government introduced a new National Security Policy (NSP) (NSP) and launched a

Funded by the European Union

ONLINE RADICALIZATION AND WAYS TO COUNTERACT ITS IMPACT

RADILAB
GHENT UNIVERSITY

14

Countering Terrorism and Violent Extremism at Facebook: Technology, Expertise and Partnerships

Elin Salomon

Facebook, we rely on a combination of technology, people and partnerships with experts to help keep our platform safe. Even as governments, companies and non-profits have battled terrorist propaganda online, we've faced a complex question over the best way to tackle a global challenge that can proliferate in different ways, across different parts of the web.

Often analysts and observers ask us at Facebook why, with our vast datasets and advanced technology, we can't just block nefarious activity using technology alone. The truth is that we also need people to do this work. And to be truly effective in stopping the spread of terrorist content across the entire internet, we need to join forces with others. Ultimately this is about finding the right balance between technology, human expertise and partnerships. Technology helps us manage the scale and speed of online content. Human expertise is needed for nuanced understanding of how terrorism and violent extremism manifests around the world and track adversarial shifts. Partnerships allow us to see beyond trends on our own platform, better understand the interplay between online and offline, and build programmes with credible civil society organisations to support counterterrorism at scale.

Proactive Efforts at Facebook: Technology and Human Expertise

Deploying Artificial Intelligence (AI) for counterterrorism is not as simple as flipping a switch. Depending on the technique, you need to carefully curate databases or have human beings code data to train a machine. A system designed to find content from one terrorist organisation may not work for another because of language and stylistic differences in their propaganda. However, the use of AI and other automation to stop the spread of terrorist content is showing promise. As discussed in our most recent Community Standards Enforcement Report, in just the first three months of 2020, we removed 6.3 million pieces of terrorist content, with a proactive detection rate of 99 percent (1).

158 HANDBOOK OF TERRORISM PREVENTION AND PREPARATION

Chapter 12

Prevention of Radicalization on Social Media and the Internet

Sara Ziegler and Joseph Gyle

In the age of selfies, snaps, likes and shares, the internet and social media have transformed the way in which people communicate. In early 2019, global internet penetration reached 57%, or 4.8 billion users, and the overall number of mobile social media users reached 47%, or 3.2 billion people.¹ This means that people are able to share ideas, communicate and interact more readily than ever before, including with audiences on the other side of the world. Terrorist groups have certainly leveraged these new mechanisms and platforms for communicating amongst themselves and to potential recruits. For example, the Islamic State of Iraq and the Levant (ISIL) has been known for producing shock videos circulated on YouTube and Twitter, and has launched new and emerging technologies and social media platforms, such as Telegram, all to promote its messages and recruit new members in cyberspace.

This chapter focuses on the prevention of radicalisation on social media and the internet in this digital age. It first reviews the relevant methods and approaches that terrorists employ to spread their propaganda and recruit online. Subsequently, it looks at some of the more common and emerging prevention and preparedness strategies which address the online space. Besides reviewing the theoretical foundations to prevent radicalisation on social media and the internet, this chapter will also draw upon specific examples, predominantly from three regions: Europe, Southeast Asia and East Africa, to illustrate what some countries are doing to tackle the problem of online radicalisation.

Keywords: radicalization, violent extremism, prevention, online, internet, social media, propaganda, counter terrorism.

3. TECHNOLOGIE EN (GEWELDDADIG) EXTREMISME



How technology can fight extremism and online harassment (Yasmin Green)

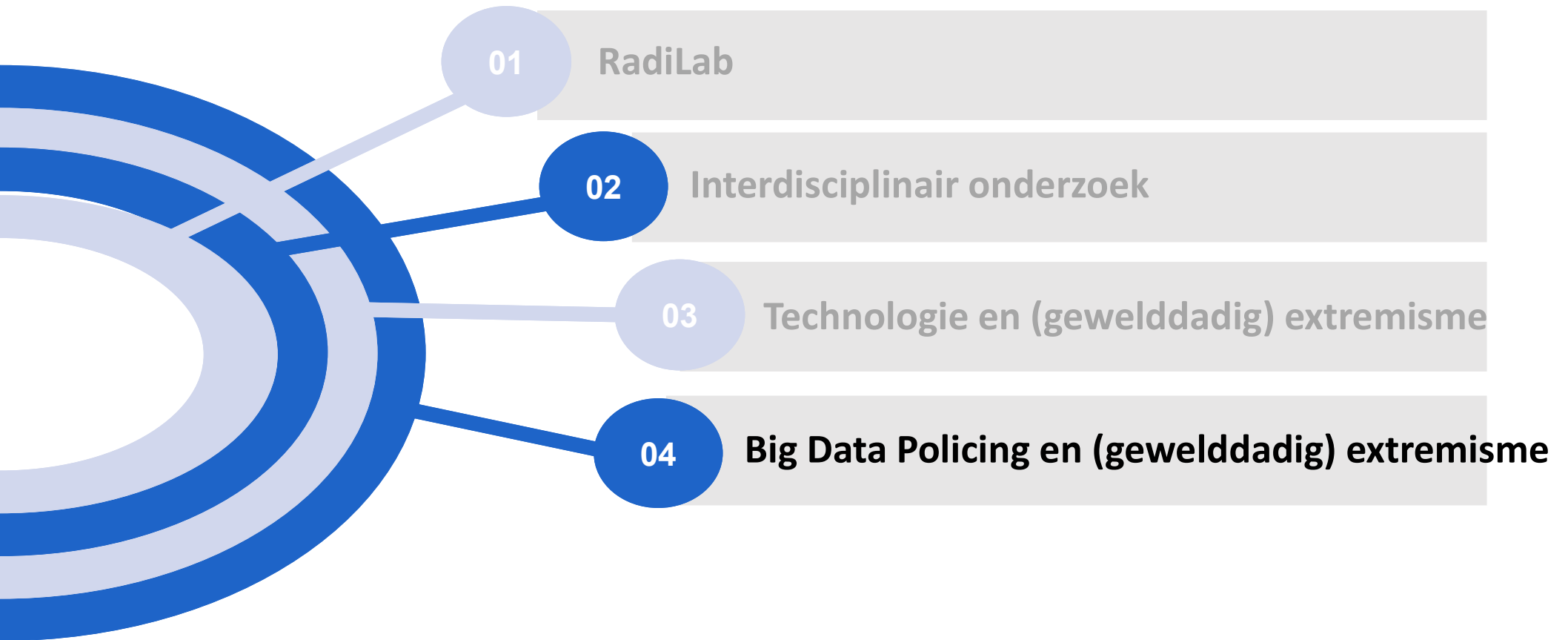
https://www.ted.com/talks/yasmin_green_how_technology_can_fight_extremism_and_online_harassment?subtitle=en&geo=fr



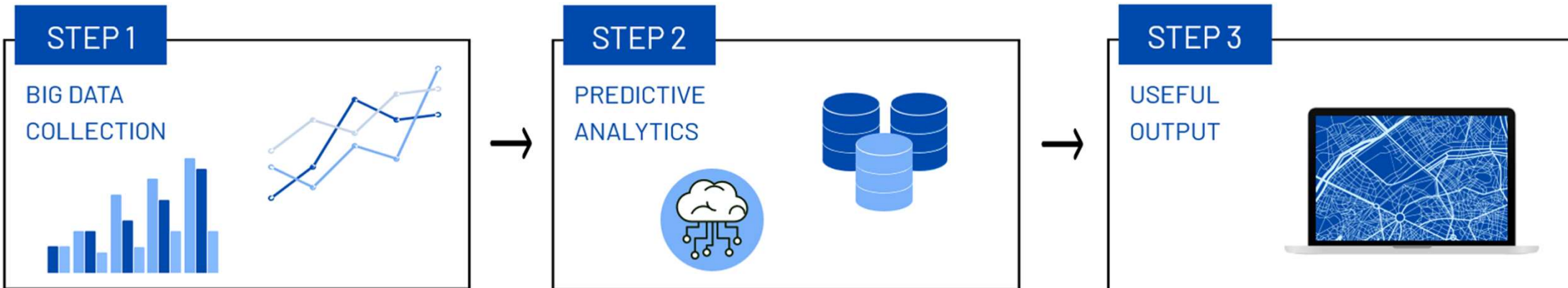
How young people join violent extremist groups and how to stop them (Erin Saltman)

https://www.ted.com/talks/erin_marie_saltman_how_young_people_join_violent_extremist_groups_and_how_to_stop_them?subtitle=en&geo=fr

INHOUDSTAFEL



5. BIG DATA POLICING



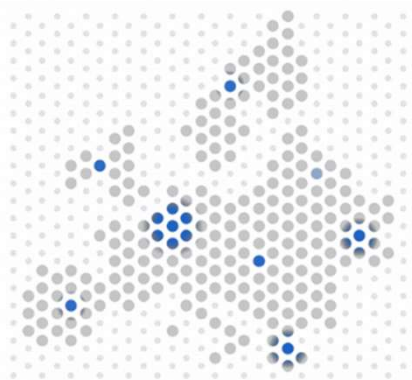
Bijvoorbeeld:

- Gegevens uit politiedatabanken
- Sociaaleconomische gegevens
- Gelegenheidskenmerken
- Nieuwe technologieën

Voorspellen **waar** en **wanneer** er een verhoogd risico is op nieuwe criminaliteit.

→ efficiënter en proactiever inzetten van politiemiddelen
→ daling van criminaliteit

5. BIG DATA POLICING



BIGDATPOL

Towards an evidence-based model for big data policing

BIGDATP

Doel = evidence-based model voor big data policing ontwikkelen



Phase 1: Inventory

- Build an open access database of big data policing initiatives
- Set up an international expert network
- Develop a typology of the existing methods
- Sample relevant cases, and original data collection



Phase 2: Analysis

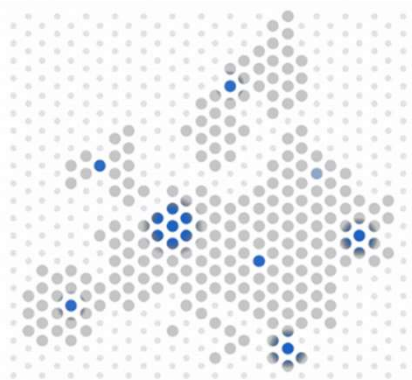
- **Track 1**
Statistical methodological analysis
- **Track 2**
Criminological and economic analysis
- **Track 3**
Legal and ethical analysis



Phase 3: Integration

- Resulting in an evidence-based big data policing model
- Tested by (quasi-)randomised controlled trials across various European cities

5. BIG DATA POLICING



BIGDATPOL

Towards an evidence-based model for big data policing

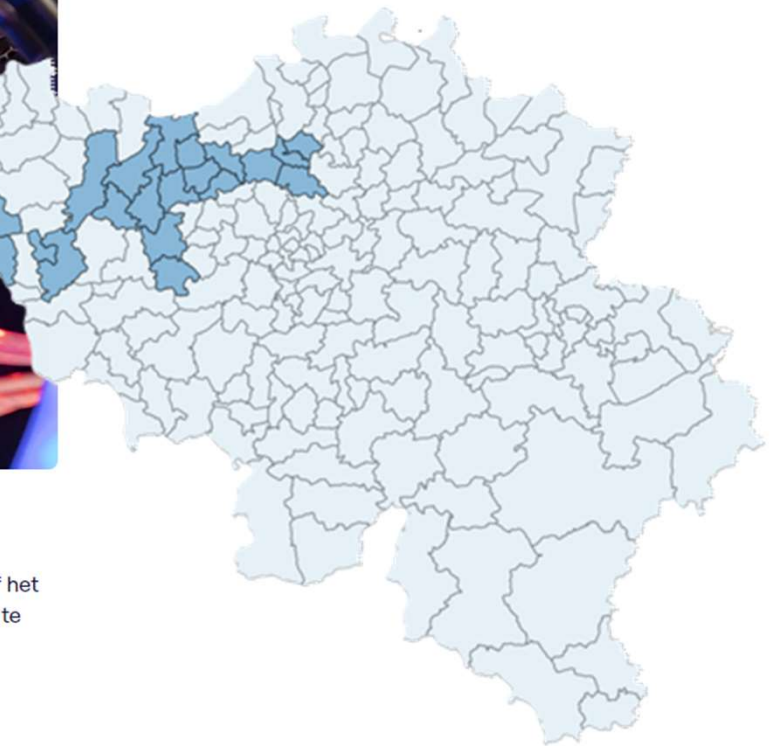
Onderzoek UGent analyseert criminaliteit in 19 politiezones met artificiële intelligentie om misdaad te voorspellen



Foto: Getty

Wetenschappers van de Universiteit Gent beginnen na de zomer aan het project BIGDATPOL. Ze gaan de criminaliteitscijfers van 19 Vlaamse politiezones uitgebreid analyseren met behulp van artificiële intelligentie om zo patronen te ontdekken. Vanaf het najaar krijgen de zones ook voorspellingen op maat, die moeten helpen om misdaden te voorkomen.

radio2, Ward Schouppe
do 25 jul © 06:23



5. BIG DATA POLICING

TOEPASSING OP RADICALISERING EN EXTREMISME?

Real Time Big Data Analytics for Predicting Terrorist Incidents

Ibrahim Toure
Department of Information Systems
University of Maryland Baltimore County (UMBC)
Baltimore, Maryland 21286
Email: itoure@umbc.edu

Aryya Gangopadhyay
Department of Information Systems
University of Maryland Baltimore County (UMBC)
Baltimore, Maryland 21286
Email: gangopad@umbc.edu

Abstract—In recent decades, terrorist groups expanded their reach and their attacks are more frequent and more lethal. In this research, we developed a set of methodologies and a software system to address various aspects of terrorism. We developed a real time terrorist incidents data collection system in [14] to gather terrorist incidents data from reliable sources. Using the incidents data, we developed a risk model to calculate the terrorist risk level of different locations. Then, we proposed a set of rules along with our risk model to predict future terrorist incidents. Finally, we developed a novel risk projection model to project the terrorist risk levels into the near future. The results show emerging patterns of terrorist attacks. Our prediction method provides high precision values of up to 96.30%, and high recall values of up to 100%. Furthermore, our risk projection model provides accurate risk values. Our methodologies can assist terrorism analysts to improve counter-terrorism measures and potentially prevent future attacks.

I. INTRODUCTION

Terrorism is a complex and evolving phenomenon. In the past few decades, we witnessed an increase in the number of terrorist incidents in the world. The security and stability of many countries is threatened by terrorist groups. Even though the probability of high lethal terrorist incidents in the United States is low, foreign terrorist groups, such as ISIS and Al-Qaeda are growing at an alarming rate. Perpetrators now use sophisticated weapons and the attacks are more and more lethal. Currently, terrorist incidents are highly unpredictable which allows terrorist groups to attack by surprise. The unpredictability is partly due to the lack of real time data and adequate risk analysis methodologies. To narrow the gap between terrorist groups and counter-terrorism experts, it is imperative to develop novel and proven methodologies along with sophisticated systems specially designed to solve terrorism related issues.

II. RELATED WORK

Many efforts have been made to collect and analyze terrorism incident data around the world. We describe a few of them in this section.

Zhen Sun et al. [10] have proposed a new event driven extraction task and four pattern-based document selection strategies. The method is applied to the terrorism event information extraction. The objective is to select a few documents as possible to construct the event related entity and relation instances.

III. METHODOLOGY

A. Risk Model

Before stepping into developing a terrorism risk projection model, we first need a risk model. We developed a risk model based on frequency and time factors.

B. Frequency Factor

For accurate risk projection, we are only interested in knowing if an incident occurs or not in a given day. Therefore,

1978-1-5000-0770-7166/\$31.00 ©2016 IEEE
Authorized licensed use limited to: University of Guelph. Downloaded on September 24, 2024 at 07:52:32 UTC from IEEE Xplore. Restrictions apply.

PLOS ONE

RESEARCH ARTICLE

Predicting terrorist attacks in the United States using localized news data

Steven J. Krieg¹, Christian W. Smith², Rasha Chatterjee¹, Nilesh V. Chawla^{1*}

1 Lucy Family Institute for Data and Society, University of Notre Dame, Notre Dame, IN, United States of America, **2** Physical Sciences Inc., Andover, MA, United States of America

* nchawla@nd.edu

Check for updates

OPEN ACCESS

Citation: Krieg SJ, Smith CW, Chatterjee R, Chawla NV (2023) Predicting terrorist attacks in the United States using localized news data. PLOS ONE 17(9): e0270981. <https://doi.org/10.1371/journal.pone.0270981>

Editor: Satishkumar V E, Hanyang University, REPUBLIC OF KOREA

Received: January 18, 2022
Accepted: June 14, 2022
Published: June 30, 2022

Peer Review History: PLOS recognizes the benefits of transparency in the peer review process; therefore, we enable the publication of all of the content of peer review and author responses alongside final, published articles. The editorial history of this article is available here: <https://doi.org/10.1371/journal.pone.0270981>

Copyright: © 2023 Krieg et al. This is an open access article distributed under the terms of the [Creative Commons Attribution License](https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Data Availability Statement: All data used in this study is publicly available from GDELT (<https://www.gdelt.net/>) and the GTD (<https://www.csis.org/gtd/>).

PLOS ONE | <https://doi.org/10.1371/journal.pone.0270981> June 30, 2022

Computers and Electrical Engineering 77 (2019) 130–147

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Big data-based prediction of terrorist attacks^a

Xi Meng^a, Lingyu Nie, Jiapeng Song

^a School of Cyber Investigation and Counterterrorism, People's Public Security University of China, Beijing, 100038, China

ARTICLE INFO

Article history:
Received 28 September 2018
Received in revised form 20 April 2019
Accepted 24 May 2019
Available online 28 May 2019

Keywords:
Hybrid Classifier
Classification
Prediction
Genetic algorithm
Optimization

ABSTRACT

An optimized hybrid classifier is proposed for the prediction of terrorist attacks. Hybrid classifier is designed using big data. It puts forward a framework that includes data collection, preprocessing, hybrid classification mining, and classifier testing as a single unit in predicting the terrorist attacks. The genetic algorithm is used to optimize the weight of each single classifier to improve the prediction accuracy of the hybrid classifier. The results reveal that the hybrid classifier is superior to the single classifier in prediction accuracy. © 2019 Elsevier Ltd. All rights reserved.

1. Introduction

The shadow of terrorist attacks has loomed globally since the 9–11 attacks. Although countries have stepped up their efforts to prevent and control them, terrorist attacks have not been far from people's lives. The Global Terrorism Database (GTD) shows that a total of 25,903 terrorist attacks took place around the world between 2000 and 2012; the average is approximately 2000 per year and more than 5 times per day [1]. There are many underlying correlations and laws in the numbers associated with terrorist attacks. If these hidden phenomena can effectively guide the construction of anti-terrorism early warning systems, they can help solve the difficult problems in counter-terrorism decision-making and conduct regular identification and prediction. This has become a research topic in many fields of informatics, as it improves the risk management and accurate warning of terrorist attacks through the use of classification technology to mine large data about terrorist attacks in depth and minimize the unknown risk of terrorist attacks.

The University of Maryland built the GTD as an open-source collection that includes data sets from the 1970s to 2014 on global terrorist activity. The database has collected and coded approximately 140,000 terrorist incidents worldwide from 1970 to 2014 and includes information about the timing, location, use of weapons and targets, number of casualties, and identifiable responsible parties. The average terrorist attack contains up to 45 messages, where the one with the most has more than 126. GTD provides researchers with comprehensive, reliable, and open-source data, and helps uncover the underlying structure behind terrorist attacks. For example, reference [2] is a data source based on the GTD's latest terrorist attacks in India that analyzes the type and number of attacks related to the attack organization. Reference [3] divides the terrorist attacks in GTD into transnational events and domestic events, analyzes and compares the impact of the both, and finds that transnational terrorism will bring more negative impact on a country's economic growth than domestic terrorism.

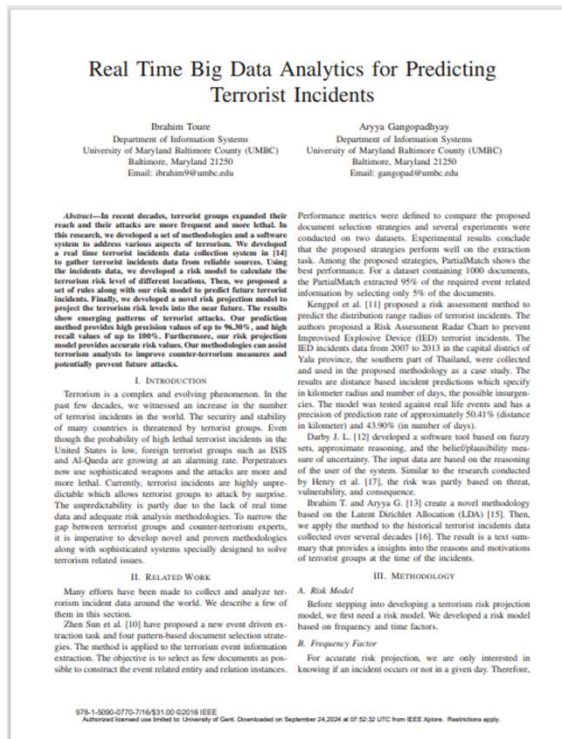
^a This paper is for CAER special section 30-ha. Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. G. Kamini-Garbatá.

* Corresponding author.
E-mail address: mengxi@pku.edu.cn (X. Meng).

<https://doi.org/10.1016/j.compeleceng.2019.05.011>
0045-7966/© 2019 Elsevier Ltd. All rights reserved.

5. BIG DATA POLICING

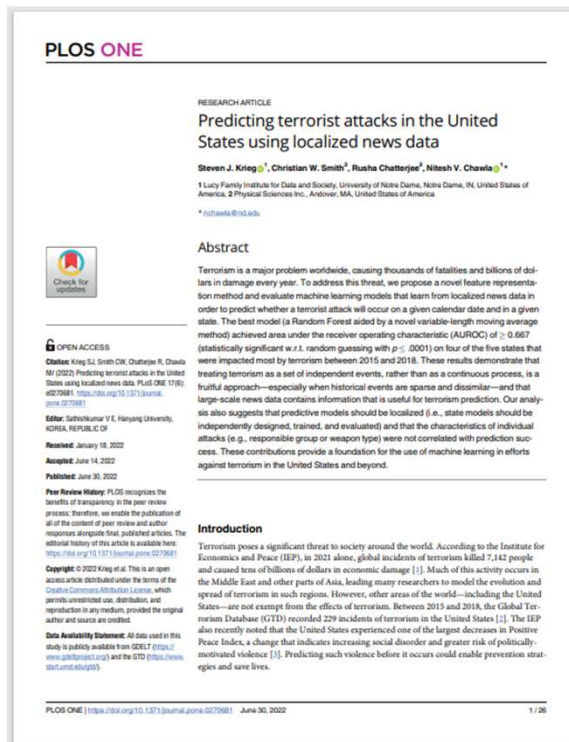
TOEPASSING OP RADICALISERING EN EXTREMISME?



- Datacollectie systeem: verzamelt in real-time data van nieuwsbronnen (ivm. incident, tijdstip, ...)
- Voorspellingsmodel voor terroristische aanslagen obv:
 - Risicomodel
 - Risicoprojectie-model
 - Gewogen risicomodel

5. BIG DATA POLICING

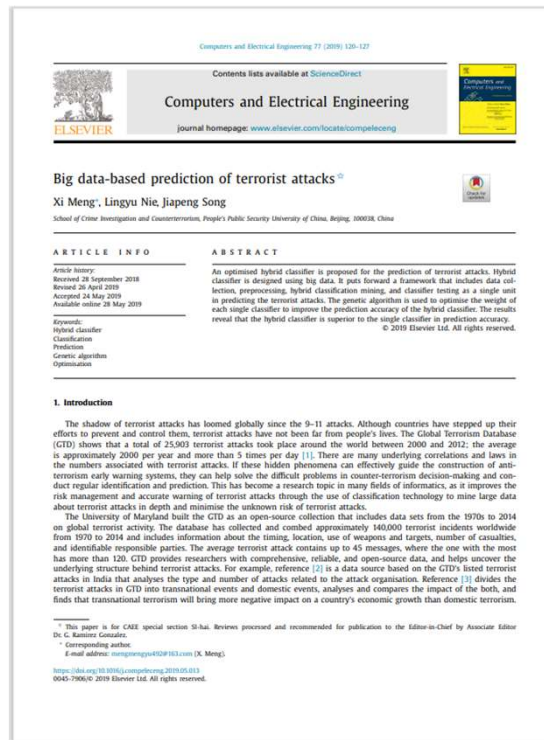
TOEPASSING OP RADICALISERING EN EXTREMISME?



- Dataverzameling
 - Global Terrorism Database (GTD)
 - Gelokaliseerde nieuwsgegevens uit de VS
- Machine learning-algoritmen
 - Voorspelt of er op dag X en locatie Y een terroristische aanslag zal plaatsvinden

5. BIG DATA POLICING

TOEPASSING OP RADICALISERING EN EXTREMISME?



- Dataverzameling
 - Global Terrorism Database (GTD)
- Gegevensverwerking
 - Data cleaning, integratie, conversie, reductie
- Mixed/hybride classifier en data testing
 - Combinatie van 4 algoritmen om terroristische aanslagen te voorspellen

JOIN OUR NETWORK

- LinkedIn page BIGDATPOL



- www.bigdatpol.com

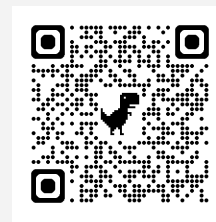


- Wim.Hardyns@UGent.be

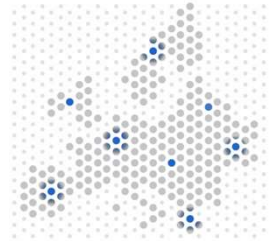
- LinkedIn page RadiLab



- www.radilab.ugent.be/en



- Wim.Hardyns@UGent.be



BIGDATPOL

Towards an evidence-based
model for big data policing





**GHENT
UNIVERSITY**