PT

# PERSPECTIVES ON TERRORISM

VOLUME XIX, ISSUE 1

MARCH 2025

A JOURNAL OF THE INTERNATIONAL CENTRE FOR COUNTER-TERRORISM

PT

PERSPECTIVES ON TERRORISM

*A journal published by*

ICCT International Centre for Counter-Terrorism

*in partnership with*

Universiteit Leiden

HANDA CSTPV
The Handa Centre for the Study of Terrorism and Political Violence

# About

## Perspectives on Terrorism

Established in 2007, *Perspectives on Terrorism* (PT) is a quarterly, peer-reviewed, and open-access academic journal. PT is a publication of the International Centre for Counter-Terrorism (ICCT), in partnership with the Institute of Security and Global Affairs (ISGA) at Leiden University, and the Handa Centre for the Study of Terrorism and Political Violence (CSTPV) at the University of St Andrews.

## International Centre for Counter-Terrorism

The International Centre for Counter-Terrorism (ICCT), founded in 2010, is a think-and-do tank based in The Hague, Netherlands. We provide research, policy advice, training and other solutions to support better counter-terrorism policies and practices worldwide. We also contribute to the scientific and public debates in the fields of counter-terrorism and countering violent extremism, notably through our publications and events.

## Institute of Security and Global Affairs

The Institute of Security and Global Affairs (ISGA) is a scientific institute specialising in security issues. ISGA is embedded in the Faculty of Governance and Global Affairs of Leiden University. ISGA originated from the Centre for Terrorism and Counterterrorism (CTC) and the Centre for Global Affairs, and today focuses on multidisciplinary research and education within the international scientific field of security studies.

## Handa Centre for the Study of Terrorism and Political Violence

The Handa Centre for the Study of Terrorism and Political Violence (CSTPV), based at University of St Andrews, is dedicated to the study of the causes, dynamics, characteristics and consequences of terrorism and related forms of political violence. Founded in 1994, the Centre is Europe’s oldest for the study of terrorism.

# Licensing and Copyright

## Licensing and Distribution

## Disclaimer

The International Centre for Counter-Terrorism does not take any responsibility for the contents of articles published in the journal, and all such responsibility lies with the author(s).

The opinions expressed in the articles are solely for the author(s), and the International Centre for Counter-Terrorism may not agree with such opinions in part of in full.

ISSN: 2334-3745

# Editorial

## Editorial Team

## Associate Editors

## Editorial Board

## Steering Board

## Contact

Email: pt.editor@icct.nl

# Table of Contents

## Words of Welcome

## Research Articles

## Research Notes

## Resources

# Words of Welcome

Dear Reader,

We are pleased to announce the release of Volume XIX, Issue 1 (March 2025) of *Perspectives on Terrorism* (ISSN 2334-3745). This Open Access journal is a joint publication of the International Centre for Counter-Terrorism (ICCT) in The Hague, Netherlands; the Handa Centre for the Study of Terrorism and Political Violence (CSTPV); and the Institute of Security and Global Affairs (ISGA) at Leiden University. All past and recent issues can be found online at https://pt.icct.nl/.

*Perspectives on Terrorism* (PT) is indexed by JSTOR, SCOPUS, and Google Scholar, where it ranks No. 3 among journals in the field of Terrorism Studies. *Jouroscope*™, the directory of scientific journals, has listed PT as one of the top ten journals in the category "free open access journals in social sciences", with a Q1 ranking. Now in its 19th year of publication, PT has close to 8,000 registered subscribers and many more occasional readers and website visitors in academia, government, and civil society worldwide. Subscription is free and registration to receive an e-mail of each quarterly issue of the journal can be done at the link provided above. The Research Articles published in the journal's four annual issues are fully peer-reviewed by external referees, while Research Notes and other content are subject to internal editorial quality control.

In the first article of this issue, James Page examines key details about Hamas' drone-related innovations, and draws implications for the future threat posed by violent non-state actors who can or might employ drones and related technologies. Next, Stephane Baele, Lewys Brace, and Elahe Naserian demonstrate how computer vision methods—including unsupervised deep clustering and supervised object identification—can be successfully applied to strengthen the study of extremist and violent political actors' online ecosystems. In the following article, a team of authors—Jade Hutchinson, David Yuzva Clement, Ruxandra M. Gheorghe, Lorraine Kellum, and Alexander Shuttleworth—explore the role of online misogyny and its psychological appeal to children and adolescences in digital media environments, and offer recommendations for addressing children's exposure to online extremist content. And in our last research article, Leoni Heyn examines the digital convergence of distinct extremist milieus involved in the Patriotic Union's December 2022 plot to overthrow the German government.

In our Research Notes section, Sarah Carthy and Yannick Veilleux-Lepage describe a pedagogical approach designed to enhance data collection skills using open-source data amongst students studying social movements and political violence. Our Resources Section begins with an extensive bibliography on Critical Infrastructure Security (Prevention, Preparedness, and Response to Terrorist Attacks) compiled by Associate Editor Judith Tinnes. Then our Book Review Editor Joshua Sinai provides a comparative overview of three recent books that focus on similar and different aspects of the psychology of terrorism. And finally, the issue concludes with several brief announcements about *Perspectives on Terrorism* from the Editorial Team. This issue of the journal has been produced in collaboration between James Forest and Anna-Maria Andreeva, with considerable assistance from Evi Konstantinopoulou, for which we are very grateful.

Prof James Forest, Editor-in-Chief

PT PERSPECTIVES ON TERRORISM

Research Article

# Drones and the Hamas-led Attack of 7 October 2023: Innovation and Implications

James M. Page*

Volume XIX, Issue 1
March 2025

ISSN: 2334-3745
DOI: 10.19165/2025.8488

**Abstract:** The Hamas-led attack against Israel on 7 October 2023 marked an important watershed in non-state actor/terrorist capability with its sophisticated and integral use of innovated drones in concert with related technologies as part of a combined arms assault. Although combined arms are typically associated with conventional forces, closer attention to Hamas-led forces' combined arms use demonstrates that terrorist groups are increasingly able to employ them to considerable effect. Hamas-led forces' combined arms use differs from ISIS' preceding use in important respects, including drones' central and integral role, the drone-related innovations demonstrated, and its particularly devastating effects. Hamas-led forces demonstrated two key drone innovations: (1) the use by a non-state actor of small drones to precisely strike sensitive, high-value defences with a novel drone-delivered munition (featuring smoke-emission/target marking and delayed detonation); (2) the use of drones as a central part of a combined-arms assault by a non-state actor. A further possible innovation is the first use of a particular modification to (small commercial) drones by a non-state actor to help enable them to evade electronic countermeasures. Hitherto, important details about Hamas' drone-related innovations, and the significant implications arising from them, have remained substantially unaddressed. Therefore, this article endeavours to fill these lacunae. Consequently, conclusions are drawn regarding the threat posed by Hamas-led forces and other non-state actors who can or might employ drones and related technologies, and what might be done to effectively address them. Moreover, because these technologies and associated training and techniques are likely to continue to rapidly proliferate.

**Keywords:** Drones, Hamas, combined arms, terrorism, counter-terrorism

* *Corresponding author: James M. Page, Durham University. E-mail: james.page@durham.ac.uk*

# Introduction

Drones[1] played a leading, and often daring, role in the 7 October 2023 Hamas-led[2] surprise attack against Israel (termed by Hamas "Al-Aqsa Flood"[3]). Consequently, considerable political,[4] media,[5] and scholarly attention[6] followed. A severe attack by a terrorist[7] or insurgent group using drones against a state had long been 'feared' by analysts,[8] academics,[9] media,[10] policymakers,[11] and members of the public.[12] The attack was triply shocking and significant because (a) it caught off-guard arguably the world's leading drone state[13] [14] that is also a leader in counter-drone technology,[15] (b) the attack was savagely conducted by a terrorist group,[16] and (c) drones had a leading, integral, *and* central role.[17] Furthermore, Israeli Defence Force (IDF) drones neither forewarned of the attack nor were they able to help bring it under swift control. (However, IDF drones later proved helpful in pursuing assailants.[18]) Moreover, on 7 October 2023, IDF air-defence and associated counter-drone technology proved largely ineffectual despite their sophistication.[19]

Particularly concerning are what Hamas-led forces were able to achieve on 7 October 2023 with innovation[20] and novelty,[21] including with drones and related technologies. This was further to the support these terrorist groups[22] are known to have received largely from Iran,[23] including for Hamas' drone programme, as part of a collection of proxy forces that possess growing transnational influence.[24] Consequently, the question arises: how did Hamas-led forces employ drones and related technologies that day, and what are the implications of this, including for preventing and combatting them? The attack's political significance is underlined by its having resulted in the third largest recorded loss of life from a single terrorist attack, and the largest loss of life in a single attack against Israel since its modern (re-) establishment, and by being the deadliest known terrorist attack assessed by the number of fatalities per capita.[25] Furthermore, it occurred despite Israel possessing cutting-edge counter-terrorism,[26] drone,[27] and counter-drone capabilities[28,29] that, combined, might have been considered to have protected Israel from an attack of the size, scale, and scope of that on 7 October 2023- but did not.

Considering this question - and the issues it raises - reveals that Hamas-led forces demonstrated the ability to execute offensive operations utilising small ground units employing small drones in a combined arms assault. This constitutes a major step in Hamas' and associated forces' capability that others, including various terrorist groups, may now seek to emulate.

Leo Blanken et al. have recently argued that "Hamas' surprise operation [on 7 October 2023] … is best understood as a non-state version of a raid" and involved "strategic" and "doctrinal surprise." Regarding the latter, they assert: "Hamas achieved this by combining many elements of what the military refers to as a multi-domain operation – and did so with a level of precision, coordination, and planning that shocked observers." These are significant points. Nonetheless, I argue that it was not only Hamas that was part of the 7 October attack; personnel from other groups participated, too. Also, although Blanken et al. refer to the US Department of Defence's (US DoD) conceptualisation of "multi-domain operation[s] [MDO]" regarding non-state actor drone use that in turn refers to "combined arms", both MDO and combined arms (as defined by the US DoD) are considerably less analytically precise, informative, and revealing than the more specific conceptualisation of combined arms developed and employed in this article that is drawn from historical usage.[30] This conceptualisation is also more specific than that offered by Kerry Chávez and Ori Swed regarding the 7 October 2023 attack and helps to identify its significance more specifically. I also argue, in effect, that Hamas-led forces' use of combined arms has implications that go beyond those entailed in Blanken et al.'s definition of "special operations".[31]

Austin C. Doctor and James I. Walsh have importantly observed “militant[t]…combined arms capability” involving drone use by ISIS in Iraq and Syria.[32] However, their use of the term “combined arms” is rather broad and equated by them with “theatre air attacks to support ground force operations” and “close air support”, as conceptualised by Robert Pape.[33] Consequently, I find Hamas-led forces on 7 October 2023 demonstrated a considerably more sophisticated capability than what Doctor and Walsh or Thomas Maurer[34] have termed “combined arms” regarding ISIS. Hamas-led forces’ combined arms assault[35] comprised: indirect fires utilising rockets, missiles, and possibly loitering munitions;[36] and direct and indirect fires utilising drones, powered paragliders, and sea and ground units. Indeed, by various measures, Hamas-led forces demonstrated substantial sophistication and achieved considerable tactical and strategic effects despite significant limitations.

Two of the most important innovations demonstrated by Hamas-led forces on 7 October 2023 were: (1) the use of a novel drone munition enabling precision strikes against IDF observation and communication towers, which were key to the assault (and arguably its success); (2) the use of combined arms by a terrorist group, in which drones possessed a central and integral role. To date, no other terrorist group has demonstrated combined arms capability in which drones had such a critical role and to such political effect.

Detailed attention to Hamas-led forces’ 7 October 2023 assault also further reveals the importance of the threat posed by smaller drones and loitering munitions, including from non-state actors, that in the scholarly literature, and more broadly, have received considerably less attention than state-employed Medium Altitude Long Endurance (MALE) drones (such as the Predator).[37] Furthermore, it shows that the use of these technologies can also occur on a large scale, result in large numbers of dead and wounded (including civilians) with high-profile results, [38] and have a major political effect when used by non-state actors.[39] These aspects underline the serious threat and challenge these technologies now pose, including to states with advanced air-defence, including counter-drone, capabilities. Moreover, although technologically based defences and countermeasures will need to be improved against all drone-types and loitering munitions, the 7 October attack paradoxically demonstrates the need for *less* reliance on high-technology to combat them and re-establish deterrence. Nonetheless, improvements in counter-drone and counter-loitering munitions technology are clearly necessary.

## Article Outline

To respond to the above questions and issues concerning Hamas-led forces’ use of drones and related technologies on 7 October 2023, this article proceeds in three parts. In doing so, it endeavours to separate drone-related developments of enduring importance from those that are ephemeral. This is important because counter-drone and counter-loitering capabilities are becoming increasingly important and challenged as drone and loitering munition development and use, including by non-state actors, rapidly develops. Indeed, with the 7 October 2023 attack, drone use as part of combined arms conducted by non-state actors has become increasingly evident, sophisticated and lethal. This stands in notable juxtaposition to the United States’,[40] among a growing number of other states’,[41] desire to effectively employ drones to address terrorist threats (in addition to those of a more conventional character[42]). Consequently, clarity and precision regarding these respective threats, and what can and ought to be done about them, are at a premium.

As a detailed official account of events on 7 October 2023 has yet to emerge, and the few extant accounts providing a detailed reconstruction of events lack sufficient focus on Hamas-led forces’ and IDFs’ use of drones and related technologies,[43] Part I provides an overview utilising a wide range of open sources, including: official statements, video footage, news media articles, videos and documentaries, analytical, policy and scholarly articles.

These have been carefully pieced together and cross-checked wherever possible. This constitutes an important evidential basis and contribution to understanding what unfolded that day and preceding it and reveals significant synchronisation and coordination in Hamas-led forces' assault, including their use of drones and other related technologies. It appears unlikely that Israel will hold a public enquiry fully disclosing what unfolded on and prior to 7 October 2023, which underlines the pertinence of this approach.

Accordingly, this article does not aim to recreate or explain every detail of what occurred; as in all accounts of war and conflict, gaps exist in our understanding of events. Nonetheless, important analysis and conclusions may still be drawn from extant evidence as is often necessary. Part II addresses Hamas-led forces' drone use innovations and novelty, and related implications, which includes detailed articulation and analysis of Hamas-led forces' employment of combined arms and its limitations. Part III considers the efficacy of Hamas-led forces' drone use on 7 October in detail and discusses what can be learned from it, followed by the conclusion.

## Part I: Hamas' and Associated Forces' Drone Use on 7 October

At approximately 6 a.m.[44] (local time) on 7 October 2023, the initial phase of the Hamas-led attack against Israel commenced. Substantial preparations preceded it; some assailants were disguised as farmers and approached Israeli border defences to check whether IDF foot patrols were nearby.[45] The Hamas-led assault near Kerem Shalom, the most southerly border crossing between Israel and Gaza, reportedly began at 5:50 a.m., when the BBC reported[46] a Hamas commander posted images, and at Kibbutz Be'eri, when Hamas-led fighters were filmed (with a time-stamp) approaching it.[47]

At approximately 6:20 a.m.,[48] the first of an enormous barrage of rockets, missiles, mortars, drones, and possibly loitering munitions was launched against Israel by Hamas-led forces,[49] in what may be regarded as the main commencement of the assault. It is estimated that this initial barrage numbered approximately 2,500 rockets, mainly al-Qassam, and lasted approximately twenty minutes.[50] [51] The initial salvo of this barrage was probably an attempt to: (a) overwhelm Israel's Iron Dome air defence system (widely regarded as one of the most capable);[52] (b) over-stimulate wider Israeli defences; and (c) clear a path for and cover Hamas-led assaults against border locations to maximise shock and sow confusion among defenders or potential defenders. [53]

Concurrent with the initial salvo (and in some locations before and after), Hamas-led forces approached and, in some cases, assaulted Israeli border defences. The fourteen visually confirmed[54] border breach points effected by Hamas-led forces were distributed roughly evenly along the length of the Israel-Gaza border (Israel claims there were approximately 29 border breach points[55]). Initial breaches were made by between 200[56] and 400[57] fighters, either through forcing open gates (e.g. near[58] Kisufim crossing), or by cutting fencing (e.g. near[59] Kerem Shalom crossing and near[60] Nir Oz), or by blasting (e.g. near[61] Be'eri and at Erez[62] crossing[63]).[64] Therefore, these breaches were synchronised with the initial salvo, even if the precise timing of each breach differed, apparently for maximum shock effect. As will be detailed shortly, this is also consistent with a combined arms assault.

Several analyses note that, as a first step, at some border locations small modified commercial drones were employed by Hamas-led forces to drop novel munitions on armed Israeli manned and unmanned observation and communication towers in a coordinated and broadly synchronised manner;[65] four of five IDF defence posts that were filmed being attacked by Hamas featured drones being used to do so. [66] This is thought to be the first time Hamas used drones in this role.[67] It meant unusual activity detected by Israeli agents could not be effectively disseminated to alert and/or activate Israeli border defences,[68] and sensors and remotely operated machine guns in some towers were rendered inoperable.

Analysed footage indicates that over 100 small drones were involved in Hamas' assault [69] and were launched from various locations, and flown into Israel.[70] The numbers are difficult to confirm provided the circumstances and as Israel has not released a detailed account of what unfolded on 7 October; however, it is highly likely that significant numbers of such drones were employed given their utility and extant reports. Meantime, cameras along the Israeli border were targeted by snipers, apparently to further reduce Israel's defences' efficacy.[71]

Reports have also emerged, including video footage, of modified small commercial (DJI and Autel)[72] drones dropping munitions directly on Israeli troops and tanks early in the Hamas-led assault. The former occurred at the IDF base at Nahal Oz,[73] and the latter against one of Israel's most advanced tanks, a Merkava IV Main Battle Tank (MBT),[74] near the Kisufim border crossing.[75] An armour-piercing munition appears to have been drone-delivered in the latter strike. Hamas-released footage, apparently of the latter, features a DJI Matrice 600 drone with what appears to be a modified RPG munition.[76] These strikes appear to have helped enable the breaching of Israeli defence lines in force, and the latter militated against a formidable mobile armoured response to counter such penetrations in the immediate and wider area. Hamas-affiliated media channels have featured another drone type, a Radiolink AT10 II; however, confirmatory evidence of its use on 7 October has not yet emerged.[77]

It is within the above events and associated actions that the most important innovation concerning drone use on 7 October occurred; drone use in combination with other specific actions and (closely related) weapons, which been characterised as "combined arms"[78] by Kerry Chávez and Ori Swed in their detailed article,[79] and others such as Mark Cancian of the Center for Strategic and International Studies, Michael Knights of the Washington Institute in interviews,[80] and the Soufan Center in a briefing report.[81] This will be assessed in further detail after more details regarding what unfolded on 7 October 2023 are presented, facilitating in-depth discussion and analysis.

Significantly, once Hamas-led forces breached the Israeli border fences, 'elite' 'Nukhba' elements proceeded to assault IDF outposts and bases, whence they mostly killed, and in some cases captured, IDF troops and disabled IDF communications and other substantial technological capabilities.[82] Typically, smaller assault forces first concentrated on IDF outposts and bases before attacking civilian dwellings in Israel. Subsequently, Hamas-led assault elements proceeded to other targets deeper into Israel, including sites of strategic national importance such as the Israeli Unit 8200 signals intelligence and fusion centre at Urim.[83] Detailed visualisation of the geography and major locations of civilian deaths can be seen here.[84]

## *Synchronisation and Further Details about the Attack*

The synchronisation of Hamas-led forces - a key aspect of their assault and directly relevant to combined arms - was considerably dispersed over a large geographical area. Further details and evidence of this follow.

Hamas-led forces employed drones to strike Israeli border defences as missile, rocket, and possibly loitering munition salvoes began at approximately 6:20 a.m.[85] This includes, for example, Kibbutz Kisufim,[86] that was assaulted by Hamas-led forces at approximately 6:35 a.m., shortly after the combined barrage began; Hamas-led forces forced open a border fence gate, entered Israel, and subsequently attacked targets.

At Kibbutz Be'eri, Hamas-led forces arrived at 5:55 a.m.,[87] and after the initial barrage, during which they infiltrated the area,[88] commenced their assault at approximately 6:55 a.m.[89] The first shots from this assault were heard at the Nova music festival,[90] the site of the single largest loss of life on 7 October. Therefore, Hamas-led forces used the initial barrage as cover and commenced their main assault on the Kibbutz, as assaults in other locations were unfolding, maximising impact and militating against a swift and robust Israeli response. During the next few hours, Hamas-led forces converged [91] on this area from the north and south,[92] guided by motorised paragliders that had been launched together with early missiles, rockets and possibly loitering munition (MRLM) salvoes.[93]

At 7 a.m., Hamas-led forces attacked Kfar Aza kibbutz, near Nahal Oz that also involved powered paragliders to guide assault forces.[94] At approximately the same time, Hamas forces attacked the largest Israel-Gaza border crossing at Erez,[95] causing extensive damage[96] and enabling numerous fighters to enter Israel.[97]

At 7:19 a.m., Hamas forces were recorded as having penetrated Zikim base[98] from the sea; fighting broke out shortly afterwards.[99] Motorised paragliders were also in the area and were among those earliest recorded to be launched beneath MRLM salvoes.[100] Not far from either Zikim or Erez, at Netiv HaAsera, the Hamas-led attack began with powered-paraglider-borne[101] Hamas fighters,[102] approximately three[103] to six[104] of whom landed in the settlement and began killing. Other assailants later arrived on foot,[105] possibly from or near the breached Erez crossing. At 7:30 a.m.,[106]attacks occurred on the Kerem Shalom kibbutz[107] and the Sufa kibbutz,[108] approximately five kilometres from one another.

Hamas-led forces eventually penetrated approximately 25 kilometres into Israel and attacked Ofakim.[109] On the way, a special Hamas unit successfully assaulted[110] the sensitive and strategically important Israeli 8200 unit signals intelligence and fusion centre at Urim,[111] which was an especially embarrassing blow to the IDF (as were reports that it had ceased eavesdropping on militant networks a year earlier).[112] Targeting of it, and the ability of Hamas-led forces to penetrate this high-value target, was a clear demonstration of the intelligence gathering and planning that went into the 7 October attack and informed its efficacy.

Hamas has claimed that in the barrage preceding the ground assault it employed approximately 35 modified versions[113] of the al-Zouari surveillance drone.[114] These modifications meant it was a loitering munition.[115] Purportedly, they were launched either from the open (as portrayed in their online released video)[116] or from covered structures.[117] However, so far, it has not proven possible to obtain independent evidence or corroboration of these launches.[118] Notably, these loitering munitions can be harder to spot and intercept than rockets or other missiles because they can fly at a lower trajectory and in the littoral[119] or seam between where ground forces operate and jet bombers.[120] Their modification suggests that, as in earlier versions of the al-Zouari drone, these loitering munitions possess surveillance capabilities.[121] Although unconfirmed, these could have helped warn if Israeli forces were in positions along the route that Hamas planned to penetrate the border. Therefore, and as Hamas has claimed, they may have been used to "facilitate[e] the crossing" of Hamas terrorists "into Gaza".[122]

It is also possible that Shehab-2 loitering munitions[123] were launched on 7 October as part of Hamas-led forces' barrages from residential buildings. However, so far, confirmatory evidence of this has not emerged. Notably, these munitions have since been targeted by IDF, as has a leading Hamas commander of its aerial array, Atsam Abu Raffa, who was reportedly responsible for such capabilities.[124] Hamas has published pictures of a supposed drone coordination centre; however, its existence has yet to be verified.[125]

If modified al-Zouari drones or modified Shehab-2 loitering munitions were employed, they might have helped to "clear" further, lower levels of airspace of Israeli drones and manned aircraft that may have been used to defend against them *and* generated intelligence, surveillance, and reconnaissance (ISR), target acquisition (TA), and strike options. Notably, loitering munitions, drones, and missiles can be difficult to electronically jam, depending on their sophistication (as has been seen in Ukraine[126]). If IDF did detect them, they could have added to the strain on IDF air defences, such as Iron Dome, including detection and targeting functions and ready supplies of missiles. Should Hamas or other terrorist groups use such munitions in the future as part of a similar attack, it could prove even more destructive and difficult to repel.

## Part II: Hamas' Drone-Related Innovations and their Implications

According to Don Rassler, Hamas has run a drone programme since c. 2003 with substantial technical support from Iran's Iranian Revolutionary Guard Corps (IRGC).[127] [128] Therefore, Hamas' drone programme is notably older than the drone programmes of most states that are assessed to currently possess one, although their respective scope and scale often differ.[129] Significantly, Hamas has used commercial drones[130] and loitering munitions for military operations since at least 2018 and 2021, respectively,[131] although reports exist of Hamas operating drones over Israel from Gaza in 2012,[132] and intensifying use in 2014.[133] Consequently, it has considerable experience in drone and loitering munition use including in combat conditions.

As Yannick Veilleux-LePage and Emil Archambault have stated, prior to the 7 October attack, Hamas' drone use involved "a variety of types of attacks", as well as drone types and targets. The latter included IDF vehicles, Iron Dome batteries, and a claimed attack against the Israeli Ministry of Defence in Tel Aviv. They note that, Hamas' drone use has neither demonstrated a clear developmental path nor consistent success, regarding which they offer three possible explanations: technical and tactical immaturity, a lack of effectiveness, and prioritising propaganda value.[134] Notably, the IDF began striking Hamas' nascent drone capability before Hamas had used drones in combat operations, i.e. reportedly in c. 2003,[135] which may have been significant in affecting Hamas' drone programme. Together, these details point to substantial improvements in Hamas': drone capability, including significant advances in their technical and tactical capacity; evident success in drone and possibly loitering munition use; and Hamas' keen attention to propaganda value, for example, regarding videos affiliated forces released on social media featuring and celebrating their drone and related technology use on 7 October.

The 7 October attack did not emerge without indication or preparations; prior to it, Hamas utilised drones, missiles, and rockets to test and strike Israel's defences, sometimes intensively. In early May 2021 (and to that date), in a foretaste of what was to occur on 7 October, the largest barrage of missiles was launched by Hamas into Israel, reportedly temporarily overwhelming Israel's renowned Iron Dome air defence system.[136] According to Abu Obaida, the spokesman for Hamas's military wing (al Qassim Brigades), preparations for the 7 October attack began in 2021, when it started to closely study Israel's tactics and strategies.[137] Iran's leadership has sent mixed messages regarding its possible involvement in the 7 October attack. As Phillip Smyth has stated, "no 'smoking gun' has emerged of direct Iranian involvement in or greenlighting of the October 7 attacks", yet, as he notes, Iran "has always maintained significant sway over its [proxy] network", including Hamas.[138]

In the months leading up to the attack, Hamas conducted ground observation[139] and flew drones to reconnoitre close[140] to the Israeli border. By June 2023, Hamas had produced planning documents, instructions, and maps for dissemination to its ground forces.[141] Hamas also attempted to mask its intentions, for instance, by disguising operatives to operate among farmers[142] and downing IDF drones in the area,[143] thereby reducing (but not completely stopping) the IDF's ability to detect significant changes in Hamas's activity. This may also have helped deter the IDF from more closely inspecting the areas used to mass and launch forces into Israel, out of concern for provoking reaction and possible drone losses. This is not unlikely regarding the atmosphere and prevailing views[144] among Israel's political and military leadership.[145]

In the days and weeks prior to 7 October, Hamas conducted[146] various operations[147] to erode and test[148] Israel's border defences, including attacking observation balloons[149] in the areas that were later assaulted, practising approaching border posts,[150] and stockpiling equipment.[151] Hamas' complex tunnel systems under Gaza were undoubtedly used to enable this, too, for example to infiltrate fighters and supplies to locations proximate to the border.[152] During this formative period, unrest in the West Bank acted as a decoy, effectively diverting Israeli troop deployments and their attempts to address this.[153]

## *Instances of Innovation*

The Hamas-led 7 October attack on Israel has been characterised by leading terrorism scholar Professor Audrey Kurth Cronin as "an old-fashioned attack with hang gliders, motorbikes, bulldozers, explosives."[154] However, the attack involved: powered paragliders and drones for ISR and TA; drones for direct fires, including use of a novel explosive freefall munition, or bomblet, dropped by drones on key IDF border defences; the novel combination of powered paragliders and drones under cover of indirect fires employing rockets, missiles, and likely loitering munitions; and these in concert with small-unit based ground manoeuvre. Consequently, the attack possessed more advanced characteristics and thus implications (as will be discussed shortly) than Cronin's comment suggests or that many analyses have so far identified or clearly articulated.

Regarding the question posed above: "how did Hamas-led forces employ drones and related technologies" on 7 October, "and what are the implications of this, including for preventing and combatting them?" this logically leads to the question: "what more precisely were the innovations that Hamas-led forces demonstrated on 7 October?" In response, considering Part I and the related analysis above, the munition used by Hamas-led forces-operated small drones to attack observation and communication towers – key IDF border defences - constitutes an important innovation.

As assessed from multiple published videos that feature Hamas-led drone strikes on these targets, it is evident that the drone-delivered bomblet/munition used to strike these defences emitted smoke after hitting the target and incorporated a considerable delay prior to detonating/exploding. Two main facilities follow from these features. First, the emitted smoke after hitting the aimed for target clearly facilitates target-marking (and was insufficient for a smoke screen). The use of smoke-releasing munitions to mark targets is long-established. This feature also provided a clear indication of the crosswind(s) the targets were subject to, regarding their significant height and exposure that might divert the munition from its aiming point, which made this feature particularly apt and notable. This feature would also enable targeting correction, for example by a subsequent drone to drop another munition with more accuracy on the target after the wind drift became evident because of the initial munition use, i.e. with correction. This is also a well-established practice in warfare, for example by artillery.[155] Second, the delayed detonation enabled the drones to move particularly close to the target and get away swiftly after dropping the munition so that the explosion would not damage the drone or back-up drones. Again, this feature has already been used in munitions. What makes this munition novel is that it is the first known recorded example of a munition with these combined features that was apparently designed for and clearly launched from a drone by a non-state actor in combat, and against such sensitive military/security targets. On 7 October, it proved potent in combination with the small drone platform, including because it was able to evade IDF defences.

The use of innovated small commercial drones to directly attack observation towers is not novel.[156] This can be observed regarding the use of small commercial drones modified by ISIS to drop munitions on Iraqi military positions in 2017.[157] It can also be identified in the use of modified drones (turning them into loitering munitions) by Ukrainian armed forces to attack a Russian observation tower in March 2023.[158] Therefore, non-state and state actors, respectively, have innovated drones before to strike such targets. The level of coordination demonstrated by Hamas-led forces that day in their (combined arms) assault on Israel had not been demonstrated prior by another terrorist group or non-state actor as will be demonstrated shortly.

A further apparent innovation has been identified in some of the small DJI Phantom drones that Hamas-led forces employed on 7 October. These drones appear to have incorporated modifications to their settings, enabling them to avoid electronic countermeasures. According to *DroneSec*, which examined footage of their use that day:

> *DJI drone icons appear on the left-hand-side of the screen, showing a 'Land' and 'Home point' icon, with the 'Return to Home' icon greyed out. This could signal the operator has disabled RTH-mode, a common counter-counter operational security measure.*

This may help to explain the ability of Hamas-led forces' drones to operate effectively on 7 October, despite advanced Israeli electronic warfare capabilities, which has been a considerable source of curiosity.[159] An additional factor appears in the disclosure in December 2023 that:

> *Israel had at least one [counter-drone] system on the Gaza border on Oct. 7 specifically designed to counter drones, but it was not yet operational. The final stages of testing were scheduled a few days after the surprise attack, according to Sentrycs, which developed it.*[160]

Regarding other non-state actor use of these modifications, no other recorded examples have been found although other modifications have been made, for example by ISIS.[161] State actors have been observed using such modifications, for example Russian and Ukrainian state forces earlier in the ongoing Russo-Ukrainian war (2022-).[162]

## *Hamas' Combined Arms Use*

Various comments have occurred regarding Hamas' coordinated use of drones combined with other offensive actions during the 7 October attack on Israel, however, so far it has not received in-depth analysis regarding it or its implications.[163] Perhaps the most detailed extant analysis is that by Kerry Chávez and Ori Swed, who observe that (1) Hamas' forces appeared to operate like a (conventional) army, particularly in their use of a "massed and combined arms approach,"[164] and that (2) although earlier similar endeavours were pioneered by ISIS, Hamas' actions on 7 October differ because Hamas' forces demonstrated two innovations. Therefore, while Chávez and Swed draw important attention to the matter of combined arms, they do not note the innovations articulated above, nor do they go into detail about Hamas-led forces' use of combined arms with drones. These represent significant lacunae that this article aims to address, among others.

Regarding the first point Chávez and Swed note, Thomas Maurer's research is helpful because it details ISIS' use of combined arms. He states ISIS "organized [weapons] into categories, [employed] purposeful combination of these forces in keeping with the concept of combined arms combat, and [utilized] hierarchical command and control executed by experienced commanders." Maurer further notes that "ISIS combat groups combined the elements of formation and firepower as well as movement and mobility." [165] Therefore, for clarity it is worth considering what constitutes "combined arms".

In its contemporary conception, combined armes can and has been dated from the latter part of the First World War.[166] Jonathan House[167] identifies its existence several years earlier in Major Gerald Gilbert's, *The Evolution of Tactics* published in 1907. The latter is significant because it pertains to a context where non-state actors were of major concern,[168] and because combined arms are currently almost exclusively associated with state forces, contrary to what unfolded on 7 October 2023. Combined arms are largely associated with conventional forces because of their reputation for complexity, the difficulty of competently conducting them, and the level of organisation and training required.[169] Quite recently, combined arms have also been observed in earlier historical periods stretching back to ancient history, indicating increasing awareness of it but also considerable variation in understanding what it entails.[170]

Consistent with what William S. Lind, Jonathan House, and latterly, Stephen Biddle have asserted, in essence "combined arms" is the use of various combat arms and weapons in concert to maximise overall efficacy and mitigate individual weaknesses.[171] It usually requires that the actions an enemy would take to defend against one element of combined arms use would result in vulnerability to another,[172] and, typically, both direct and indirect fires are employed combined with considerable force manoeuvre. In addition to concern about its strategic implications,[173] recently the concept of combined arms has seen an emphasis on information operations, including propaganda,[174] and even AI.[175]

Although Maurer does not explicitly note ISIS's use of direct and indirect fires and manoeuvres *in concert or synchronicity*, he does state direct and indirect fires and manoeuvres were combined and "coordinat[-ed] "taking into account time and space" by ISIS (pre-2018).[176] Thus, Maurer's assessment of ISIS's use of combined arms is broadly congruent with the combined arms' essence, although less specific. Maurer notes ISIS's use of drones for ISR but does not discuss drone use for launching direct strikes in this context.[177] This provides an important comparison with Hamas-led forces' innovative use of drones as part of combined arms whereby drones were used for direct and indirect fires, pre-attack ISR, and almost certainly TA. Moreover, drones were used in concert with other arms as part of a synchronised assault of substantial size, scope, and sophistication. Doctor and Walsh have asserted ISIS employed "combined arms" in Syria, which they equate with "theatre air attacks to support ground force operations" and "close air support", as conceptualised by Pape.[178] However, they do not remark upon key elements of combined arms, such as synchronicity, nor do they provide clear details of ISIS's combined arms use, including how drones were employed. Indeed, ISIS is not known to have conducted a combined arms attack with drones possessing such an integral role or on such a scale as Hamas-led forces did on 7 October.

Regarding Chávez's and Swed's first point about Hamas-led forces' use of drones on 7 October, they state that Hamas "simulat[-ed] mass with off-the-shelf drones that can be deployed in multiple ways, including being equipped with bombs and repurposed into weapons of war." Part I of this article provides substantial detail that corroborates this observation. It also furnishes further insight that it was the combination of drones, including those employing direct fires, together with other munitions (including those used for indirect fires using rockets, missiles, and possibly loitering munitions) that "simulated mass" and not only drones. This is an important corrective.

Chávez's and Swed's second point is that on 7 October, Hamas was responsible for "pioneering a new combined arms model with commercial drones that is unusual for terrorist organizations."[179] While evidence corroborates this, they do not specify why and how. Neither do they clearly conceptualise the "combined arms model" they refer to nor note its limitations. They are nonetheless correct that the description and label of "combined arms" are less frequently applied to terrorists or insurgents.

As Part I above details, Hamas-led forces were able to take advantage of the difficulty air defences often have in detecting small drones before they deliver strikes against targets, including defences.[180] Regarding small drone use and combined arms, Hamas-led forces conducted drone strikes using small drones with a novel munition and in concert with, and under cover of, a barrage of massed indirect fires comprising missiles, rockets, and possibly loitering munitions. Concurrent with this, and at multiple locations (as detailed in Part I), Hamas-led forces breached and assaulted Israeli border defences at multiple strategic points with small units in a synchronised manner, including with follow-up forces involving substantial command-and-control.

Hamas-led forces subsequently infiltrated Israeli territory and attacked a variety of locations, including military and civilian military installations. This has been well documented (see Part I). Powered paragliders launched in concert with the initial indirect fires salvo, were subsequently observed helping to coordinate Hamas-led forces' manoeuvre. They also attacked Israeli targets from the air, and 'dismounted' fighters assaulted civilian targets (such as at Netiv HaAsera).[181] In addition to paragliders, during the assault drones were also used for ISR (and prior to it), TA and strike. An unmanned balloon has also been claimed by a Hamas-affiliated account, however, it has not been confirmed.[182]

Accordingly, Hamas-led forces "pioneer[-ed] a new combined arms model with commercial drones that is unusual for terrorist organizations" and demonstrated a novel innovation on 7 October with the sophistication of their drone use as part of a combined arms assault, which included ISR, TA, and strike. Although paragliders were also used in these ways, Hamas-led forces' drone use was comparatively more sophisticated in these regards, both technically and in practice.

Accordingly, drones were used for direct fires and to facilitate direct and indirect fires. Drone-facilitated indirect fires, for example ISR prior to the assault and during it, almost certainly added to the pressure on Israeli air defences because further projectile salvoes were unleashed by Hamas-led forces. It is highly probable that these salvoes helped further enable Hamas-led forces' drone use and their combined arms assault. This is because Israeli air and ground defences' ability to respond was almost certainly hampered; for example, IDF took cover and was prevented from mounting a coordinated or clearly targeted response resulting from these indirect and direct fires (including by drones).

Novel counter-jamming modifications (for non-state actors) that were detected in Hamas-led forces' small modified commercial drones, enabled them to target key IDF defences, including armed border observation posts and communications towers, and IDF troops and tanks, as did their use of a novel munition when attacking the former. Representing highly significant innovations for Hamas and non-state actors, including terrorist groups, are the use of small drones, technical innovations to them, and munitions used by them, and the central role drones had in a combined arms assault. Indeed, no other terrorist group has so far demonstrated this range of capabilities, which are more usually associated with a state actor. Furthermore, no state actor has demonstrated this particular use of drones in an assault.

# Part III: Drone Use Efficacy Against Israel: What can be Learned?

## *The Efficacy of Hamas-led Forces' 7 October Drone Use*

During the assault, IDF personnel frequently did not (and arguably could not) directly combat breaches of Israeli defences in a concerted or highly organised manner. Reviewing numerous reports, including video footage of the assault, this was not least because of the need for IDF to take cover from rocket, missile (and possibly loitering munition) salvoes launched by Hamas-led forces in the initial attack, in concert with drone strikes, and static and mobile small arms fire (detailed in Part I). Therefore, rather than the 7 October attack being one of "supporting arms"[183] Hamas-led forces' combined arms assault proved especially effective in suppressing, breaching, and assaulting thinly manned high-tech static defences and overwhelming light concentrations of mobile IDF defences that were deployed that day. The specific and successful targeting of communications by Hamas-led forces using drone-launched novel munitions also meant that IDF were unable to coordinate a rapid and sufficiently robust response to repel and stem breaches in border defences and the infiltration of larger groups of Hamas-led fighters. The effect of this was to amplify the initial success of the Hamas-led attacks on Israeli border defences and the overall scale and scope of the assault (as detailed in Part I).

In consequence, the ability (and likelihood) of IDF effectively marshalling a swift response to initial Hamas-led attacks against Israeli border defences before Hamas-led forces broke through in substantial numbers, seized defences/strong-points, and fanned out - including striking civilian targets - was militated against by Hamas-led forces' use of combined arms.

Indeed, Hamas-led forces' use of combined arms, and drones as part of it, included utilising drones' strengths as an ISR, TA and strike platform against the specific defensive capabilities that IDF had developed, including as part of its high-technology border defences. Hamas-led-forces' use of rocket, missile, and possibly loitering munition salvoes during the assault provided cover for their drone use and the ground units operating them as they approached, assaulted, and in some instances held positions, and in other instances, continued to infiltrate Israel (see Part I).

If more IDF personnel had been available on 7 October, it is improbable that they could have effectively combatted this combined arms assault because of its scale and scope, including its suppressive and disorientating effects, for instance its precise targeting of key components of IDF defences, i.e. observation and communication towers, strong-points, IDF high-tech ISR, and related communications capabilities. This meant that IDF border defences, including automated weapons to detect, initially repel and enable swift reinforcement, and mobile forces such as tanks, were rendered largely ineffective. Thus, the structure of IDF defences and their vulnerability to combined arms assaults involving drones and other weapons require careful reconsideration regarding what is known to have unfolded on 7 October. This further underlines the efficacy and threat posed by Hamas-led forces evidenced combined arms capability.

Additional salvoes of rockets, missiles, and possibly loitering munitions also made it more difficult for IDF aircraft, including drones, to interdict Hamas-led forces, as did the increasing numbers of assailants that flowed through the breached defences and their subsequent manoeuvre into urban and more open terrain. Hamas-led forces' use of motorised paragliders, launched under the cover of the initial barrage, to help guide Hamas-led forces and partake in attacks, is a further innovation demonstrated by them on 7 October as part of a combined arms assault. The use of motorised (and armed) paragliders can also be regarded as potentially compensating for the potential vulnerability of drones to electronic warfare, as they can and were used to help coordinate attacks. Hamas-led forces' drones' limited strike capabilities also meant these paragliders provided additional mobile attack capability with personnel in them able to fire onto targets and to land, dismount and assault locations (such as at Netiv HaAsera),[184] as well as the propaganda effect of their use both visually and historically *vis-à-vis* "Night of the Gliders".[185]

An important aspect of Hamas-led forces' use of combined arms on 7 October is "it reinforces the shift in the dominant characteristic of war[-fare] from maneuver to decision" (alteration of war to warfare mine);[186] in the case of the 7 October assault IDF and Israel's political leadership were placed in a very difficult decision-making position where it was much less a question of manoeuvre than of deciding what to do. This was despite Israeli doctrinal, infrastructure, equipping, policy and political investments in technology-driven ISR and quick-reaction capabilities,[187] [188] which proved inadequate. Hamas-led forces demonstrated detailed knowledge of Israeli defences, which were directly and effectively targeted by them on 7 October,[189] including communications within defence structures on the border and the communications towers struck by drones. This extended to the highly important and sensitive signals intelligence facility at Urim.

The apparent limited objectives of the Hamas-led attack on 7 October (within an unlimited political and military goal of the eradication of Israel that Hamas has asserted numerous times before and since the 7 October assault[190]) included demonstrating their capability to: shock, maim, torture, kill, and capture Israelis; undermine the IDF's reputation; destabilise the Netanyahu government (that is highly critical of Hamas and Iran); obtain propaganda; and take military and civilian hostages for political and military concessions. These were in broad alignment with and further to Hamas-led forces' use of combined arms. That Hamas-led forces were unable to seize and hold territory for more than approximately one day indicates the significant limits of Hamas-led forces' combined arms capability. However, although they were limited in their ability to seize and hold territory, they were still able to penetrate deep into Israel, strike sensitive facilities, and capture and remove a large number of hostages. Indeed, it appears hostages were used instead of holding territory (after doing so) to try to obtain political concessions. Thus, although Hamas-led forces' actions indicated the use of limited war, this occurred as part of the war that Hamas has expressed in unlimited terms.

## *What Can Be Learned?*

Hamas-led forces' demonstration of a potent if "unorthodox" combined arms capability, with drones and possibly loitering munitions at its centre, breaks new ground. This includes, in terms of non-state actors, capabilities that have been demonstrated so far, including in the ongoing conflict between Israel and Iranian proxy forces. Hamas-led forces' development of drone-related combined arms capability is occurring as part of the shift[191] that is unfolding, involves drones moving from being almost exclusively employed by states to find, fix, and, in some cases, strike terrorists, insurgents, and other non-state actors,[192] to their utilisation by terrorists and insurgents to attack state forces and civilians.[193] This shift has been characterised as democracies using drones to combat terrorism to its inverse.[194]

The seizure of hostages by Hamas-led forces, further to their combined arms assault instead ,of protracted land-seizure may be regarded as a substitution, albeit a distasteful one, which is highly morally, ethically, and legally objectionable. Arguably, this has shown considerable political efficacy in the short to medium term. It also provides a counterpoint to Hamas' objections to Israeli settlements in occupied areas.[195] Consequently, Hamas may be able to translate combined armed use (with drones having a central role) into a more strategic and political tool. However, in the medium and long term it may attract strong and counter-productive responses.

Hamas appears to have learned from ISIS' technical drone innovation and drone use, including its innovation in drone munitions, although the precise links between them are not yet fully clear. Ukrainian and Russian armed forces also probably provided a significant source of innovation inspiration to Hamas[196] and possibly technical insights towards the alteration of DJI commercial drone safety configurations. However, more details are needed to establish why and how Hamas innovated as it did. It remains likely that other terrorist and insurgent groups will also seek to emulate the combined arms capability and elements thereof that Hamas-led forces demonstrated on 7 October.

Beyond Israel-Gaza, there is growing evidence that non-state actors are seeking to develop drone-related capabilities, including to target highly trained state forces. Perhaps the latest example of this is in the Red Sea, where Houthis have launched loitering munitions and drones against international shipping, including naval forces from the US, UK, France, Netherlands, and others.[197] This strongly suggests that states will need to become far more vigilant regarding the threat such groups with drone and loitering munition capabilities pose. As Hamas-led forces' drone-related capabilities proved central to the efficacy of their attack on Israel on 7 October, that possessed highly advanced drone and counter-drone and counter-airborne munition capabilities, this serves as an important warning to other states.

Regarding non-state actors' combined arms capability - including drones, loitering munitions, and missiles- it is conceivable that this could develop rapidly especially with state assistance, including in contexts in which training can be provided, weapons and weapon systems can be transported or smuggled, and expertise and experience communicated or transferred. This can be inferred from the development of Hamas' drone and related technologies capability.[198] Therefore, vigilance will be needed regarding non state actors' training facilities and weapon supplies, including so-called "dual use" technologies,such as commercial drones.

In addition to drone-related developments in Ukraine,[199] improved counter-drone capabilities against state and non-state actors appear increasingly essential. They are no longer niche capabilities and are necessary across a wide range of armed forces, including for basing and the manoeuvre of forces at small-unit level and above. Although Israel was in the process of deploying and integrating technology to assist its troops to target and shoot down drones, missiles, rockets and possibly loitering munitions, this came too late to prove effective.[200]

In the future, the use of drones by small units to infiltrate an adversary's territory is likely to be an area of substantial threat because small drones can act as a significant force-multiplier, including to enhance the lethality of their attacks, and help to preserve small units by forewarning of defences and/or interdiction by larger or superior forces. In turn, this markedly increases the damage non-state actor assault teams could cause state, non-state actors, and civilians in material, political, military, and psychological terms.

Hamas' and associated forces' use of drones in combined arms has also demonstrated the limitations of border walls, fences, and wider defence complexes even with high technology enhancements. Arguably, it has shown the need for troops to be deployed to defend territory or strategic and tactical points in considerable depth and with more resilient communications links that were in place in Israel on 7 October. Although this runs counter to the assumptions and tenets incorporated in Israel's 2015 military strategy and the "Decisive Victory" operational concept - and despite the temptation to regard this as more of a glitch than a fundamental challenge – these will need to be revisited and reappraised. This is especially so given: previous failure (2006), the scale and scope of the 7 October failure, and increasing Hamas and other terrorist and other non-state actors' technological capabilities, including drones, loitering munitions, rockets, and missiles. Moreover, now that the 7 October attack has proven to be a successful operation and template. This also implies that Israel will need to keep a closer eye on training camps and possible preparations for other such attacks against it, as will other states.

## Conclusion

On 7 October 2023, Hamas-led forces demonstrated substantial drone-related innovations. From a technical standpoint, the most novel innovation was not of a drone itself but that of a drone-delivered munition which possessed two main novel features: (1) the emission of smoke upon hitting the target area, and (2) delayed detonation. These combined attributes in a drone-delivered munition have not been identified as in previously employed by either a terrorist or non-state actor. These munitions were employed highly effectively by what appear to be modified small commercial drones against Israeli high-technology observation and communications towers. The observation towers incorporated sensors and interlinked machine guns but proved unable to effectively detect or combat small drones. The smoke emitted by and delayed explosion of the novel drone-delivered munitions utilised by Hamas-led forces proved effective in achieving drone precision strikes and drone survivability. The former feature also offered the possibility of corrected drone strikes if crosswinds significantly affected the accuracy of the initial strikes, which could have proven particularly helpful given the combined arms context in which synchronisation is highly important.

A further possible novelty is also evident in the apparent incorporation of technical modifications to DJI Phantom small drones used in strikes against Israeli targets that would have helped prevent them being jammed. This is the first time such a modification has been detected in non-state actor-employed drones. Together, these constitute substantial innovation in non-state and terrorist drones and their use because neither one nor all these innovations has so far been identified in other non-state actor and terrorist drones or their use.

The most important drone-related innovation and capability that Hamas-led forces demonstrated on 7 October was the use of combined arms, in which drones had a central and integral role. While some may regard their combined arms use in historical terms as unorthodox, it is not in view of the historical origins and context of the concept. Hamas-led forces' combined arms involved and exhibited shrewd and synchronised use of missile, rocket, and possibly loitering munition-based mass, in concert with small drone precision strikes (enabled through novel innovations to small drones). The assault occurred across various geographically and functionally interlinked defence points in close succession. The overall size and scale of the combined arms assault by Hamas-led forces may also be regarded as a novel feature; it is almost certainly the largest recorded combined arms assault in combat by a non-state actor. It was also able to comprehensively breach sophisticated bespoke air and ground defences with devastating tactical, operational, strategic, and political effects.

Consequently, the Hamas-led assault on 7 October 2023 constitutes substantial innovation according to both measures of "innovation" asserted by, on the one hand Williamson Murray, and on the other Theo Farrell and Michael C. Horowitz, as detailed above. That is, and respectively, changes in capability that have occurred in a period of peace (i.e. in preparation for the assault), and in a major change in the conduct of warfare. It also draws attention to what Nina Kollars regards as the overlooked area of adaptation during conflict, provided the blurring that occurs between conflict statuses and, in turn, respective leading conceptualisations of "adaptation" and "innovation".

Given the importance of at least Iranian knowledge transfer for the development of Hamas' drones and loitering munitions,[201] remaining questions about Iran's role in the 7 October attack may help spur further attention to the role and importance of what Brown et al. term institutional actors "in enabling or enhancing adaptation at the lowest level."[202]

Regarding border defences and those of sensitive sites, the direct targeting of Israel's border defences, and in particular key elements of their high technology composition (with its underpinning assumptions including light staffing), should serve as a warning to Israel and other states that such defences may prove either an insufficient deterrent or defence or both to a combined arms attack.

A combined arms attack including armed and unarmed drones and related technologies, and as a *modus operandi*, is likely to be attractive to many non-state actors and even states. While the technological and employment capabilities of terrorists and other non-state actors are rapidly improving, concerningly, counter-drone capabilities, particularly against small drones and loitering munitions, lag.[203] This adds urgency for further developing the latter. As Liran Antebi and Matan Yanko-Avikasis state, drones (and, in effect, loitering munitions) should be considered "a new layer" and should be dealt with specifically, "and not necessarily in conjunction with other aerial threats such as manned aircraft or missiles and rockets."[204]

Although respective terrorist and insurgent group drone, loitering munition, and counter-drone and counter-loitering munition capabilities are often considerably less sophisticated than those of states, the 7 October assault by Hamas-led forces demonstrated that the latter, and potentially other non-state actors, can incur serious military and political blows against states. This includes against arguably the state with the most advanced capacities fielded for defending against these technologies.[205] Although states often rely on MALE drones, for various reasons they have largely neglected the importance of smaller drones, including those utilised by small units, and counter-drone capabilities to defend against such use.[206] This is despite the increasing importance of the "littoral" or "seam" between the ground and where manned (ground-attack) jets operate.

Paradoxically, in addition to high-tech solutions, a premium should be placed on the early detection of suspicious human activity to prevent the build-up of capacities and forces for such an attack. An attack such as that on 7 October 2023 requires detailed and complex planning, so human intelligence is vital to detect it despite the difficulty in developing and sustaining it. The temptation for 'cleaner' and more calculable forms of intelligence gathering and response belies the countermeasures that state and non-state actors can take against signals intelligence and high-technology-based intelligence gathering and related forewarning. Moreover, technological innovation and adaptation are almost certain to continue, which means this dimension will see alterations in capabilities as well as opportunities that can and will be exploited by state and non-state actors alike.

*James M. Page is an Honorary Fellow in the School of Government and International Affairs, Durham University.*

# Endnotes

[1] Drones are defined in accordance with that provided by James Page: “unmanned, remote controlled powered aircraft (with varying degrees of autonomy) capable of changes in direction, height and speed, which are designed to be and typically are reusable.” This accords with Boyle’s observation in his substantial book about drones: “[a]mong the key characteristics that most drones share is that: (1) they are flown remotely: (2) they are capable of flight manoeuvres; and (3) they are typically intended to be reused, unlike missiles and other disposable projectiles.” This has important analytical and wider implications; see: James M. Page, “Loitering Munitions and Drones: The Urgent Need for Clarity,” *Royal United Services Institute*, Newsbrief, April 26, 2024, https://www.rusi.org/explore-our-research/publications/rusi-newsbrief/loitering-munitions-and-drones-urgent-need-clarity ; Michael J. Boyle, *The Drone Age: How Drone Technology Will Change War and Peace* (Cambridge: Cambridge University Press, 2020): 7-8, https://academic.oup.com/book/36688/chapter-abstract/321730595?redirectedFrom=fulltext . All accessed July 9, 2024.

[2] While Hamas was the largest group involved and is widely regarded as having planned and led the 7 October assault (with external support), other groups were also involved, including (but not necessarily limited to): Palestinian Islamic Jihad (PIJ), the second largest militant organisation in Gaza and a widely proscribed terrorist group (as is Hamas); the Mujahideen Brigades, and; Al-Nasser Salah al-Deen Brigades. See, e.g.: BBC, “How Hamas built a force to attack Israel on 7 October,” *BBC*, November 27, 2023, https://www.bbc.com/news/world-middle-east-67480680 ; USIP, “Israel-Hamas War: Comments by Hamas & PIJ,” The Iran Primer, *US Institute of Peace*, October 11, 2023, https://iranprimer.usip.org/blog/2023/oct/11/israel-hamas-war-comments-hamas-pij . All accessed July 9, 2024.

[3] This was announced in a pre-recorded message by a Hamas spokesman several hours after the attack began. See: Samia Nakhoul and Laila Bassam, “Who is Mohammed Deif, the Hamas commander behind the attack on Israel?,” *Reuters* October 11, 2023, accessed July 9, 2024, https://www.reuters.com/world/middle-east/how-secretive-hamas-commander-masterminded-attack-israel-2023-10-10/ .

[4] Seung Mim Kim and Matthew Lee, “Biden decries the ‘unconscionable’ Hamas attack and warns Israel’s enemies not to exploit the crisis,” *Associated Press*, October 8, 2023, https://apnews.com/article/israel-hamas-palestinians-gaza-rockets-airstrikes-biden-0b6abb762dabd46aa826af891591b392 ; Times of Israel, “UK PM Sunak slams ‘barbarity’ of Hamas attack on Israel,” *Times of Israel*, October 8, 2023, https://www.timesofisrael.com/liveblog_entry/uk-pm-sunak-slams-barbarity-of-hamas-attack-on-israel/; Nahal Toosi, Phelim Kine and Andrew Zhang, “China’s soft message on Hamas is part of a much bigger strategy,” *Politico*, October 12, 2023, https://www.politico.com/news/2023/10/11/israel-hamas-china-middle-east-policy-00120995 . All accessed July 9, 2024.

[5] Regarding media attention about the attack, see for example: Jordyn Beazley, “‘Israel declares war’: What the papers say about the surprise Hamas attack and its aftermath,” *The Guardian*, October 8, 2023, https://www.theguardian.com/world/2023/oct/08/israel-declares-war-what-the-papers-say-about-the-surprise-hamas-attack-and-its-aftermath ; Karl Vick, “A Surprise Attack Upends Israel and the Middle East,” *TIME*, October 8, 2023, https://time.com/6321849/israel-attack/ ; Patrick Kingsley and Isabel Kershner, “‘We Are at War,’ Netanyahu Says After Hamas Attacks Israel,” *New York Times*, October 7, 2023, https://www.nytimes.com/2023/10/07/world/middleeast/israel-netanyahu-hamas-attack.html ; Yolande Knell, Raffi Berg and David Gritten, “Israel attack: PM says Israel at war after 250 killed in attack from Gaza,” *BBC*, October 7, 2023, https://www.bbc.co.uk/news/world-middle-east-67036625.amp ; James Rothwell and Nataliya Vasilyeva, “Hamas terrorists butcher civilians as stunned Israel suffers ‘9/ moment’,” *Telegraph*, October 7, 2023, https://www.msn.com/en-gb/news/world/hamas-terrorists-butcher-civilians-as-stunned-israel-suffers-9-11-moment/ar-AA1hQGFb ; Dan Williams, “How the Hamas attack on Israel unfolded,” *Reuters*, October 7 2023, https://www.reuters.com/world/middle-east/how-hamas-attack-israel-unfolded-2023-10-07/ ; Washington Post, “Maps and videos show how the deadly surprise attack on Israel unfolded,” *Washington Post*, October 7, 2023, https://www.washingtonpost.com/world/2023/10/07/israel-gaza-timeline-videos-maps/ ; Haaretz, “Gaza Declares War: Surprise Infiltration, Massive Barrages Shock Israel; Over 250 Israelis Killed, 1,590 Wounded; Civilians and Soldiers Held Hostage in Gaza,” *Haaretz*, October 7, 2023, https://www.haaretz.com/israel-news/2023-10-07/ty-article-live/israel-under-attack-terrorists-infiltrate-from-gaza-amid-massive-rocket-barrages/0000018b-088b-dae9-adcb-abbff50f0000 . All accessed July 9, 2024. Notably, none of these leading media reports mentions drones, but rather concentrate on more familiar weapons that were more immediately in evidence, such as rockets and missiles in addition to small arms. Media attention about drones’ role in the attack followed shortly after, particularly after videos taken by Hamas of their use were published, see, e.g.: Samuel Oakford, Evan Hill, Joyce Sohyun Lee and Meg Kelly, “Videos show how Hamas achieved its unprecedented surprise attack on Israel,” *Washington Post*, October 8, 2023, https://www.washingtonpost.com/world/2023/10/08/israel-gaza-videos-border/ ; Mia Jankowicz, “How Hamas likely used rudimentary drones to ‘blind and deafen’ Israel’s border and pave the way for its onslaught,” *Business Insider*, October 10, 2023, https://www.businessinsider.com/hamas-drones-take-out-comms-towers-ambush-israel-2023-10?op=1 ; David Hambling, “How cheap drones helped Hamas ambush Israel’s sophisticated weaponry,” *Forbes*, October 9, 2023, https://www.forbes.com/sites/davidhambling/2023/10/09/how-hamas-leveraged-cheap-rockets-and-small-drones-to-

ambush-israel/; Aric Toler, “How Hamas Attacked Israel’s Communications Towers,” *New York Times*, October 10, 2023, https://www.nytimes.com/2023/10/10/world/middleeast/hamas-israel-attack-gaza.html ; Justin Ling, “The Dangerous Mystery of Hamas’ Missing ‘Suicide Drones’,” *WIRED*, October 21, 2023, https://www.wired.com/story/hamas-drones-israel-war/ ; Sean Rayment, “The danger of Hamas drone attacks,” *Spectator*, November 6, 2023, https://www.spectator.co.uk/article/the-danger-of-hamas-drone-attacks/ . These videos can be seen at: Younis Tirawi يونس @ytirawi, X formerly known as Twitter, October 7, 2023, https://twitter.com/ytirawi/status/1710622183670608064 ; SamuleBendett @sambendett, X formerly known as Twitter, October 8, 2023, https://twitter.com/sambendett/status/1711004280654635512 . All accessed July 9, 2024.

[6] In general, see, e.g.: Daniel Byman and Alexander Palmer, “What You Need to Know About the Israel-Hamas War,” *Foreign Policy*, October 7, 2023, https://foreignpolicy.com/2023/10/07/hamas-attack-israel-declares-war-gaza-why-explained/ *;* Lawrence Freedman, “What comes next in Gaza: Israel was wrong to think it could contain Hamas so easily,” *New Statesman*, October 8, 2023, https://www.newstatesman.com/world/middle-east/2023/10/israel-gaza-what-comes-next ; Matthew Levitt, “The War Hamas Always Wanted How the Group’s Attack Could Disrupt the Emerging Order in the Middle East,” *Foreign Affairs*, October 11, 2023, https://www.foreignaffairs.com/israel/war-hamas-always-wanted . Regarding drones, see e.g.: Kerry Chávez and Ori Swed, “How Hamas innovated with drones to operate like an army,” *Bulletin of the Atomic Scientists*, November 1, 2023, https://thebulletin.org/2023/11/how-hamas-innovated-with-drones-to-operate-like-an-army/ ; Liran Antebi and Matan Yanko-Avikasis, “Life and Death in the Hands of the Drone: The Small, Cheap Devices Early in the Swords of Iron War,” *INSS Insight*, No. 1772, October 26, 2023, https://www.inss.org.il/wp-content/uploads/2023/10/No.-1772.pdf . All accessed July 9, 2024.

[7] Hamas is designated as a terrorist organisation by the US, UK, Canada, Australia, Japan, Egypt, Paraguay, the EU, Organization of American States, and the United Nations. See: Linda Gradstein, “Explainer: How Hamas Ended Up on US List of Terrorist Groups,” *VOA*, February 7, 2024, https://www.voanews.com/a/explainer-how-hamas-ended-up-on-us-list-of-terrorist-groups/7478227.html; Sergio García Magariño, “What is Hamas? Seven key questions answered,” *The Conversation*, October 11, 2023, https://theconversation.com/what-is-hamas-seven-key-questions-answered-215391. Regarding labelling see: Ronit Berger Hobson and Assaf Moghadam, “Terrorism, Guerrilla, and the Labeling of Militant Groups,” *Terrorism and Political Violence,* March 9, 2023, DOI: 10.1080/09546553.2023.2183052. All accessed July 9, 2024.

[8] See, for example: Jay Mandelbaum and James Ralston, Project Leaders Ivars Gutmanis, Andrew Hull and Christopher Martin, “Terrorist Use of Improvised or Commercially Available Precision-Guided UAVs at Stand-Off Ranges: An Approach for Formulating Mitigation Considerations,” Institute for Defense Analyses, IDA Document D-3199, October 2005, https://apps.dtic.mil/sti/pdfs/ADA460419.pdf ; Ulrike Franke, “Drone Proliferation: A Cause for Concern?” *ISN*, ETH Zurich, November 13, 2014, https://www.files.ethz.ch/isn/187855/ISN_185404_en.pdf . All accessed July 9, 2024.

[9] Dennis Gormley, “Unmanned Air Vehicles as Terror Weapons: Real or Imagined?” *Nuclear Threat Initiative* Report, June 30, 2005, https://www.nti.org/analysis/articles/unmanned-air-vehicles-terror-weapons/ ; Michael J. Boyle, “The costs and consequences of drone warfare,” *International Affairs*, 89, (2013), 1-29, https://doi.org/10.1111/1468-2346.12002 ; Boyle, *The Drone Age,* Ch.5; Håvard Haugstvedt and Jan Otto Jacobsen, “Taking Fourth-Generation Warfare to the Skies? An Empirical Exploration of Non-State Actors’ Use of Weaponized Unmanned Aerial Vehicles (UAVs—‘Drones’)”, *Perspectives on Terrorism*, 14, no. 5 (October 2020), https://www.universiteitleiden.nl/binaries/content/assets/customsites/perspectives-on-terrorism/2020/issue-5/haugstvedt-and-jacobsen.pdf ; Ash Rossiter, “Drone Usage by Militant Groups: Exploring Variation in Adoption,” *Defense & Security Analysis* 34, no. 2 (April 3, 2018), 113–26, https://doi.org/10.1080/14751798.2018.1478183 ; James Rogers, “Future Threats: Military UAS, Terrorist Drones, and the Dangers of the Second Drone Age,” Matthew Willis, André Haider, Daniel C. Teletin, and Daniel Wagner (eds.), *A Comprehensive Approach to Countering Unmanned Aircraft Systems* (Kalkar, Germany: NATO Joint Air Power Competence Centre, 2021), https://www.japcc.org/wp-content/uploads/A-Comprehensive-Approach-to-Countering-Unmanned-Aircraft-Systems.pdf . All accessed July 9, 2024.

[10] See, e.g.: CBS, “NYPD scanning the sky for new terrorism threat,” *CBS*, October 29, 2014, https://www.cbsnews.com/news/drone-terrorism-threat-is-serious-concern-for-nypd/; Jack Nicas, “Criminals, Terrorists Find Uses for Drones, Raising Concerns,” *Wall Street Journal*, January 28, 2015, https://www.wsj.com/articles/criminals-terrorists-find-uses-for-drones-raising-concerns-1422494268 ; Alyssa Sims, “How do we thwart the latest terrorist threat: swarms of weaponised drones?” *Guardian*, January 19, 2018, https://www.theguardian.com/commentisfree/2018/jan/19/terrorists-threat-weaponised-drones-swarm-civilian-military-syria . All accessed July 9, 2024.

[11] See: Boyle, *The Drone Age,* Ch.5; BBC, “Warning over drones use by terrorists,” *BBC*, 12 January 2016, https://www.bbc.com/news/technology-35280402 ; UN, “Preventing Terrorists from Acquiring Weapons: Technical guidelines to facilitate the implementation of Security Council resolution 2370 (2017) and related international standards and good practices on preventing terrorists from acquiring weapons,” United Nations Office for Counter-Terrorism, n.d., accessed July 9, 2024,

https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Mar/technical_guidelines_to_facilitate_the_implementation_of_security_council_resolution_2370_2017_and_related_international_standards_and_good_practices_on_preventing_terrorists_from_acquiring_weapons.pdf .

[12] Comparatively little polling has been done regarding public perceptions about the threat of terrorist drone use. However, views have been ascertained as part of wider polling, see, e.g.: Philip Boucher, "'You Wouldn't have Your Granny Using Them': Drawing Boundaries Between Acceptable and Unacceptable Applications of Civil Drones," *Science and Engineering Ethics* 22 (2016), 1391–1418 ; UK Government, "Public dialogue on drone use in the UK," London: HMSO, 2016, https://assets.publishing.service.gov.uk/media/5a7f97a2ed915d74e622b672/drones-uk-public-dialogue.pdf ; Marina Miron, David Whetham, Margaux Auzanneau, Andrew Hill, "Public Drone Perception", Technology in Society 73, 2023, https://doi.org/10.1016/j.techsoc.2023.102246 . All accessed July 9, 2024.

[13] Regarding Israel's position as a leading 'drone power' see: Seth J Franzman, "How Israel became a leader in drone technology," *Jerusalem Post*, July 13, 2019, https://www.jpost.com/Israel-News/How-Israel-became-a-leader-in-drone-technology-595209 ; Peter Bergen, Melissa Salyk-Virk, David Sterman, "World of Drones," *New America Foundation*, July 30 2020, https://www.newamerica.org/future-security/reports/world-drones/ . Israel has been particularly secretive regarding its development of drone capability and comparatively few in-depth publications exist regarding this. Detailed sources include: Thomas P. Ehrhardt, "Unmanned Aerial Vehicles in the United States Armed Services: A Comparative Study of Weapon System Innovation," Ph.D. thesis, Johns Hopkins University, 2000, https://www.proquest.com/docview/276148273/previewPDF ; David Rodman, "Unmanned Aerial Vehicles in the Service of the Israel Air Force: they Will Soar on Wings Like Eagles," *Middle East Review of International Affairs*, 14, no. 3 (September 2010), 77-84; David Rodman, *Sword and Shield of Zion: The Israel Air Force in the Arab–Israeli Conflict, 1948–2012* (Eastbourne: Sussex Academic Press, 2013). Regarding Israel's development of drone capability and theoretical arguments, see: Moritz Weiss, "How to become a first mover? Mechanisms of military innovation and the development of drones," *European Journal of International Security*, 3, part 2, 187–210, esp. 198-201, doi:10.1017/eis.2017.15. All accessed July 9, 2024.

[14] Notably, Israel has long used drones, at times intensively, to help keep Iranian-proxy forces such as Hamas and Hezbollah at bay. See: Ehrhard, "Unmanned Aerial Vehicles in the United States Armed Services"; Rodman, "Unmanned Aerial Vehicles in the Service of the Israel Air Force"; Rodman, *Sword and Shield of Zion*. This is not least because these terrorist groups and their main sponsor have repeatedly sworn to eradicate Israel. See, e.g.: MEMRI, "Israel's Eradication – An Ideological And Practical Goal Of Iran's Islamic Revolution Regime," *MEMRI*, Special Dispatch No. 7682, September 25, 2018, https://www.memri.org/reports/israels-eradication-–-ideological-and-practical-goal-irans-islamic-revolution-regime ; Bruce Hoffmann, "Understanding Hamas's Genocidal Ideology," *Atlantic*, October 10, 2023, https://www.theatlantic.com/international/archive/2023/10/hamas-covenant-israel-attack-war-genocide/675602/. The IDF have sought drones to help prevent surprise attacks and to minimise the loss of life, for example in response to attempts to intimidate and attack Israel preceding the 1967 six-day war, the 1973 Yom Kippur war, and the Second Lebanon war in 2006. See, e.g.: Guy Laron, *The Six-Day War: The Breaking of the Middle East* (New Haven: Yale University Press, 2018); Michael B. Oren, *Six Days of War: June 1967 and the Making of the Modern Middle East* (Oxford: Oxford University Press, 2002); Simon Dunstan*, The Yom Kippur War: The Arab-Israeli War of 1973* (Oxford: Osprey Press, 2007); Insight Team of the London Sunday Times, *The Yom Kippur War* (London: iBooks, 2016); Ehrhard, "Unmanned Aerial Vehicles in the United States Armed Services"; Rodman, "Unmanned Aerial Vehicles in the Service of the Israel Air Force"; Rodman, *Sword and Shield of Zion*. All accessed July 9, 2024.

[15] See, e.g.: Tamir Eshel, "Israel's Counter-UAV Technologies: Securing the Skies," *European Security and Defence,* June 28, 2023, accessed September 10, 2024, https://euro-sd.com/2023/06/articles/31808/israels-counter-uav-technologies-securing-the-skies/; Seth J. Frantzman "Israel Is Slowly Become a Drone Superpower," *National Interest*, July 20, 2020, accessed September 10, 2024, https://nationalinterest.org/blog/buzz/israel-slowly-become-drone-superpower-165149 ; Arthur Holland Michel, "Counter-Drone Systems," 2nd Edition, Center for the Study of the Drone at Bard College, 2019, accessed September 10, 2024, https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf

[16] See, e.g.: Julia Frankel, "Israeli video compilation shows the savagery and ease of Hamas' attack," *Associated Press*, October 17, 2023, accessed July 9, 2024, https://apnews.com/article/israel-palestinians-hamas-attack-military-war-a8f63b07641212f0de61861844e5e71e .

[17] As we will see, drones were part of the initial and ongoing assault; they were also used to strike key Israeli border defences and provide intelligence before and during the assault, as well as propaganda, including as part of "information operations".

[18] Antebi and Yanko-Avikasis, "Life and Death in the Hands of the Drone: The Small, Cheap Devices Early in the Swords of Iron War"; Seth J. Frantzman, "In the war against Hamas, Israeli drones are

key. Here is why," *Long War Journal*, October 20, 2023, accessed July 9, 2024, https://www.fdd.org/analysis/2023/10/20/in-the-war-against-hamas-israeli-drones-are-key-here-is-why/ .

19 See, e.g.: Vikram Mittal, "The Challenges Of Counter-Drone Technology As Seen In Recent Conflicts," *Forbes*, October 18, 2023, https://www.forbes.com/sites/vikrammittal/2023/10/18/the-challenges-of-counter-drone-technology-as-seen-in-recent-conflicts/ ; Seth J. Frantzman, "Lasers, integration and mobility: Israel races to stop growing threat from drones," *Defense one*, May 24, 2021, https://www.defensenews.com/unmanned/2021/05/24/lasers-integration-and-mobility-israel-races-to-stop-growing-threat-from-drones/ . All accessed July 9, 2024.

20 Regarding innovation and adaptation – concepts that are often intertwined - Williamson Murray helpfully distinguishes them regarding the context in which they respectively occur. Adaptation occurs during conflict when "there is little time, but there is feedback of combat results, which can suggest necessary adaptations", whereas innovation occurs outside of conflict. Neat distinctions between conflict and non-conflict periods can be problematic regarding terrorist groups that are ostensibly involved in ongoing terrorist campaigns over many months or years (as in the case of Hamas), notably prior to the 7 October attack Hamas had agreed and were observing a ceasefire with IDF. Therefore, the period prior to Hamas-led forces' attack on 7 October can reasonably be claimed as a period of innovation rather than adaptation. A different approach is taken by Horowitz and Farrell, both of whom see innovation as a major change in the conduct of warfare, whereas adaptation involves lesser change to tactics, techniques, or existing technologies to improve "operational" performance. Nina Kollars helpfully draws attention to the importance of adaptation (during conflict) and the "less fanfare" and attention it has received. Notably, Brown et al., observe the lack of attention in the scholarly literature to "the role of institutional actors in enabling or enhancing adaptation at the lowest level." This article may help spur further attention to this dimension. See: Kyle Brown, Jonathan Askonas, and T.S. Allen, "How the Army Out-Innovated The Islamic State's Drones," *War on the Rocks*, December 21, 2020, https://warontherocks.com/2020/12/how-the-army-out-innovated-the-islamic-states-drones/; Nina Kollars, "Organising Adaptation in War," *Survival* 57 no. 6, 111–26. doi:10.1080/00396338.2015.1116158; Williamson Murray, *Military Adaptation in War: With Fear of Change* (Cambridge: Cambridge University Press, 2011), 2; Michael C. Horowitz, *Diffusion of Military Power: Causes and Consequences for International Politics* (Princeton, NJ: Princeton University Press, 2010), 22; Theo Farrell, "Improving in War: Military Adaptation and the British in Helmand Province, Afghanistan, 2006–2009," *Journal of Strategic Studies,* 33, no. 4 (August 2010), 569.

21 While innovation and novelty are closely linked, novelty can also mean something that has not occurred before and does so here. This distinguishes it from innovation, a term that is used here without implying something that has not occurred previously (although it may not have occurred in the same circumstances or resulted from the efforts of the same organisation/entity).

22 Yasmine Salam, "Hamas group explained: Here's what to know about the group behind the deadly attack in Israel," *NBC*, 10 October 2023, accessed July 9, 2024, https://www.nbcnews.com/news/investigations/hamas-know-group-deadliest-attack-israel-decades-rcna119628 .

23 Don Rassler, "Remotely Piloted Innovation Terrorism, Drones and Supportive Technology," *Combating Terrorism Center Sentinel at West Point United States Military Academy,* 2016, https://ctc.westpoint.edu/remotely-piloted-innovation-terrorism-drones-and-supportive-technology/ ; Andrew Hanna, "Iran's Drone Transfers to Proxies," *United States Institute of Peace, Iran Primer,* June 30, 2021, https://iranprimer.usip.org/blog/2021/jun/30/iran's-drone-transfers-proxies ; Dion Nissenbaum , Sune Engel Rasmussen and Benoit Faucon, "With Iranian Help, Hamas Builds 'Made in Gaza' Rockets and Drones to Target Israel," *Wall Street Journal*, May 20, 2021, https://www.wsj.com/articles/with-iranian-help-hamas-builds-made-in-gaza-rockets-and-drones-to-target-israel-11621535346 . All accessed July 9, 2024.

24 Regarding Iranian proxy forces and their relationship with these groups, see, e.g.: Ashley Lane, "Iran's Islamist Proxies in the Middle East," *Wilson Center*, September 12, 2023, https://www.wilsoncenter.org/article/irans-islamist-proxies ; Neil MacFarquhar, "The Proxy Forces Iran Has Assembled Across the Middle East," *New York Times*, October 27, 2023, https://www.nytimes.com/2023/10/27/world/middleeast/iran-proxy-militias.html ; Nakissa Jahanbani, "Reviewing Iran's Proxies by Region: A Look Toward the Middle East, South Asia, and Africa," *CTC Sentinel* 13, no. 5 (May 2020), 39-49, https://ctc.westpoint.edu/reviewing-irans-proxies-by-region-a-look-toward-the-middle-east-south-asia-and-africa/ ; Shahram Akbarzadeh, William Gourlay and Anoushiravan Ehteshami Iranian proxies in the Syrian conflict: Tehran's 'forward-defence' in action, *Journal of Strategic Studies* 46, no. 3, 683-706, DOI: 10.1080/01402390.2021.2023014 ; Stephen Johnson, "Iran Is Working Hard to Revive Anti-U.S. Operations in Latin America," *Foreign Policy*, June 1, 2020, https://foreignpolicy.com/2020/06/01/iran-venezuela-alliances-latin-america/ . All accessed July 9, 2024.

25 Daniel Byman, Riley McCabe, Alexander Palmer, Catrina Doxsee, Mackenzie Holtz, and Delaney Duff, "Hamas's October 7 Attack: Visualizing the Data," *Center for Strategic and International Studies*, December 19, 2023, accessed July 9, 2024, https://www.csis.org/analysis/hamass-october-7-attack-visualizing-data .

[26] See, e.g.: Daniel Byman, *A High Price: The Triumphs and Failures of Israeli Counterterrorism* (Oxford: Oxford University Press, 2011); Boaz Ganor, *Israel's Counterterrorism Strategy: Origins to the Present* (New York: Columbia University Press, 2021).

[27] Regarding Israel's drone capacities, see, e.g.: Michael J. Boyle, *The Drone Age: How Drone Technology Will Change War and Peace* (Oxford: Oxford University Press, 2020), 47-49, 63-68, 94,140,151-155, 162, 191-193, 237-266; Uri Sadot and Ulrike Franke, "Proliferated Drones: A Perspective on Israel," *Center for a New American Security*, May 12, 2016, https://drones.cnas.org/reports/a-perspective-on-israel/ ; Seth J. Frantzman "Why Israel Waited until Now to Reveal Armed Drones," The Jerusalem Post, July 21, 2022, https://www.jpost.com/israel-news/article-712757 ; Kerry Chávez and Ori Swed, "A Case Study On Integrating Tactical Drones: Israel," *Modern War Institute at West Point*, June 28, 2024, https://mwi.westpoint.edu/a-case-study-on-integrating-tactical-drones-israel/ . All accessed September 19, 2024.

[28] See: JTA, "Hamas' attack on Israel was the deadliest day for Jews since the Holocaust," *Jewish Telegraphic Agency*, October 8, 2023, https://www.jta.org/2023/10/08/israel/was-hamas-attack-the-bloodiest-day-for-jews-since-the-holocaust ; Aaron Boxerman, "What We Know About the Death Toll in Israel From the Hamas-Led Attacks," *New York Times*, November 12, 2023, https://www.nytimes.com/2023/11/12/world/middleeast/israel-death-toll-hamas-attack.html . All accessed July 9, 2024.

[29] Notably, drone and counter-drone capabilities have developed unevenly, including as part of the "hider-finder" dynamic, see: Antonio Calcara, Andrea Gilli, Mauro Gilli, Raffaele Marchetti, Ivan Zaccagnini, "Why Drones Have Not Revolutionized War," *International Security* 46, no. 4, 130-71, DOI:10.1080/01402390500137259. Smaller drones (which Calcara et al. do not consider in detail) have further complicated this dynamic; see, e.g.: André Haider, "Countering Unmanned Aircraft Systems," in *De Gruyter Handbook of Drone Warfare*, ed. James Patton Rogers (Boston/Berlin: De Gruyter, 2024), 399-417. Although drone and counter-drone capabilities involve different endeavours and technologies, notably leading drone states are also often leaders in counter-drone technologies, e.g., the United States and Israel, see, e.g., Boyle, *The Drone Age.*

[30] Leo Blanken, Ian Rice, and Craig Whiteside, "Al-Aqsa Storm Heralds the Rise of Non-state Special Operations," *War on the Rocks*, November 2, 2023, accessed July 9, 2024, https://warontherocks.com/2023/11/al-aqsa-storm-heralds-the-rise-of-non-state-special-operations/ . Regarding the US Department of Defense official definition and conceptualisation of US Multi-Domain Operations and combined arms as referred to by Blanken et al., see: Andrew Feickert, "Defense Primer/ Army Multi-Domain Operations (MDO)," *Congressional Research Service*, IF11409, January 2, 2024, https://crsreports.congress.gov/product/pdf/IF/IF11409; US Department of Defense, "DoD Dictionary of Military and Associated Terms," Joint Publication 1-02. Washington, D.C.: U.S. Department of Defense (DoD), January 2024, https://www.hsdl.org › c › view?docid=886178; US Department of Defense, "Joint Security Operations in Theatre," Joint Publication 3-10. Washington, D.C.: U.S. Department of Defense (DoD), 25 July 2019, Validated on 6 August 2021, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_10.pdf?ver=tWS6OVNLUUD2EOPwDE4pAw%3d%3d ; US Department of Defense, "Joint Forcible Entry Operations," Joint Publication 3-18. Washington, D.C.: U.S. Department of Defense (DoD), 11 May 2017 Incorporating Change 1 09 January 2018, Validated on 09 July 2021, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_18ch1.pdf?ver=A9WjEOdmKtKqabuKPDGu_g%3d%3d ; US Department of Defense, "Joint Land Operations," Joint Publication 3-31. Washington, D.C.: U.S. Department of Defense (DoD), 03 October 2019 Incorporating Change 2 31 March 2023, https://csl.armywarcollege.edu/content/docs/jp3_31ch2.pdf . All accessed September 20, 2024.

[31] This because Leo Blanken et al's conceptualisation of "special operations" pertains to those that are "in general… small unit actions that generate effects that directly support campaign outcomes and are often associated with bespoke training, equipment, and tactics that allow small units to achieve outsized results." However, combined arms are not necessarily or even typically limited to "special operations". Notably, what constitutes "outsized results" is also open to broad interpretation. Furthermore, "outsize results" may not be what some special operations forces are intended or used for, such as discrete intelligence-gathering, liaison, training and advising, and where overall results that they importantly contribute to are difficult to clearly assess and quantify. Therefore, this conceptualisation of "special operations" may not be the most apt. See: Blanken et al. "Al-Aqsa Storm Heralds the Rise of Non-state Special Operations."

[32] Craig Whiteside and Vera Mironova have observed ISIS' use of drones in 2017, and drawn attention to the importance of this, however, they do not note combined arms use with drones by ISIS. Craig Whiteside and Vera Mironova, "Adaptation and Innovation with an Urban Twist," *Military Review*, November-December 2017, 79-85.

[33] Austin C. Doctor and James I. Walsh, "The Coercive Logic of Militant Drone Use," *Parameters*, 51, no. 2 (Summer 2021), 73-84, 81, doi:10.55540/0031-1723.3069. A similar argument is made by them in: Austin C. Doctor and James I. Walsh, "The Militant Drone Playbook," *War on the Rocks,* August

12, 2021, https://warontherocks.com/2021/08/the-militant-drone-playbook/ ; Robert A. Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca, NY: Cornell University Press, 1997). All accessed September 20, 2024.

[34] Thomas Maurer, "ISIS's Warfare Functions: A Systematized Review of a Proto-state's Conventional Conduct of Combat Operations," *Small Wars & Insurgencies* 29, no. 2, 20 March 2018, 229-244, 229, DOI: 10.1080/09592318.2018.1435238 .

[35] Specific details of what combined arms entail are discussed in detail later in this article. It may be helpful to note that here it is employed congruent with the following conceptualisation offered in this article: "'combined arms' is the use of various combat arms and weapons in concert to maximise overall efficacy and mitigate individual weaknesses. It usually requires that the actions an enemy would take to defend against one element of combined arms use would result in vulnerability to another, and typically both direct and indirect fires are employed combined with considerable force manoeuvre. In addition to concern about its strategic implications, recently, the concept of combined arms has seen an emphasis on information operations, including propaganda, and even AI."

[36] Unlike drones, loitering munitions are designed to be non-reusable and non-recoverable munitions.. See also, e.g.: Page, "Loitering Munitions and Drones: The Urgent Need for Clarity;" Brennan Deveraux, "Loitering Munitions in Ukraine and Beyond," *War on The Rocks*, Commentary, April 22, 2022, https://warontherocks.com/2022/04/loitering-munitions-in-ukraine-and-beyond/ ; Ingvild Bode and Tom F.A. Watts, "Loitering munitions: legal rules for autonomy in weapon systems," *ICRC Humanitarian Law & Policy* Blog, June 29, 2023, https://blogs.icrc.org/law-and-policy/2023/06/29/loitering-munitions-legally-binding-rules-autonomy-weapon-systems/ . This is more specific than many extant conceptualisations of drones and loitering munitions, the advantage of which is that it is more precise and acknowledges the different physical attributes and resultant political implications of drones, loitering munitions, ballistic missiles and other technologies, as well as their relatedness. All accessed July 9, 2024.

[37] This is the focus of, for instance, the long running "drone debate". Drones that fit in this widely used categorisation include the US Predator and Reaper and the Turkish Bayraktar TB-2. Regarding drone classification, for a simple, helpful, and widely applied example based on NATO standards see: Dan Gettinger, "The Drone Databook," *Bard Center for the Study of the Drone*, October 2019, iv-v, accessed July 9, 2024, https://dronecenter.bard.edu/files/2019/10/CSD-Drone-Databook-Web.pdf . Also see more broadly, e.g.: Roland E. Weibel, "Safety Considerations for Operation of Different Classes of Unmanned Aerial Vehicles in the National Airspace System," (master's thesis, Massachusetts Institute of Technology, 2002), https://dspace.mit.edu/bitstream/handle/1721.1/30364/61751476-MIT.pdf?sequence=2 . regarding the "drone deate" see, e.g.: Avery Plaw, Matthew S. Fricker and Carlos R. Colon, *The Drone Debate: A Primer on the U.S. Use of Unmanned Aircraft Outside Conventional Battlefields*, Lanham, MD: Rowman & Littlefield.

[38] Regarding the importance of the use of small drones and loitering munitions recently in Ukraine see, e.g.: James M. Page, "Drones in Ukraine: Claims, Concerns and Implications," *Royal United Services Institute (RUSI) Newsbrief,* June 10, 2022, accessed July 9, 2024, https://rusi.org/explore-our-research/publications/rusi-newsbrief/drones-ukraine-claims-concerns-and-implications ; Dominika Kunertova, "The war in Ukraine shows the game-changing effect of drones depends on the game," *Bulletin of the Atomic Scientists* 79, no. 2, 95-102, DOI: 10.1080/00963402.2023.2178180 ; Dominika Kunertova, "Drones have boots: Learning from Russia's war in Ukraine," *Contemporary Security Policy* 44, no. 4, 576-591, DOI:10.1080/13523260.2023.2262792.

[39] Brown et al., "How the Army Out-Innovated The Islamic State's Drones," offer a particularly well-informed and insightful article regarding the threat posed by non-state actor drone use (particularly smaller than MALE drones) against state actors and what has been done, especially by the US, to counter them since c. 2011. Several other authors have offered informative assessments of the terrorist threat posed by drones from non-state actors, including designated terrorist groups. However, Hamas' attack, of which drones were an integral part, was unprecedented in scale, scope and high-profile political effect. Arguably, it also calls for a rethink, at least by Israel if not others, of their counter-drone and counter-loitering munition endeavours. Regarding the non-state actor drone threat, see, e.g.: Kerry Chávez and Ori Swed, "Off the Shelf: The Violent Nonstate Actor Drone Threat," *Air & Space Power Journal,* Fall 2020, 29-43; Ryan Jokl Ball, The Proliferation of Unmanned Aerial Vehicles: Terrorist Use, Capability, and Strategic Implications," *Lawrence Livermore National Laboratory*, LLNL-TR-740336, October 17, 2017; Robert, J. Bunker, *Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2015); Dennis Gormley, "Unmanned Air Vehicles as Terrorist Weapons: Real or Imagined?" *Nuclear Threat Initiative,* June 30, 2005. All accessed September 20, 2024.

[40] Regarding the US use of drones for counter-terrorism, helpful overviews regarding US targeted killing campaigns are provided by: Avery Plaw, Matthew S. Fricker and Carlos R. Colon, *The Drone Debate: A Primer on the U.S. Use of Unmanned Aircraft Outside Conventional Battlefields* (New York: Rowman & Littlefield, 2016). 27-50; Boyle, *The Drone Age*, 55-97. Regarding the US's continued use

and even reliance on drones, for example, after its withdrawal from Afghanistan in the summer of 2021, see: James M. Page, "Zawahiri's Assassination Proves the War in Afghanistan Is Far From Over," *The National Interest,* September 11, 2022, accessed July 9, 2024, https://nationalinterest.org/print/feature/zawahiri's-assassination-proves-war-afghanistan-far-over-204691 .

41 See, e.g.: Joshua A. Schwartz, Matthew Fuhrmann, and Michael C Horowitz, "Do Armed Drones Counter Terrorism, Or Are They Counterproductive? Evidence from Eighteen Countries," *International Studies Quarterly* 66, no. 3 (September 2022), https://doi.org/10.1093/isq/sqac047 .

42 James M. Page, "Zawahiri's Assassination Proves the War in Afghanistan Is Far From Over," *National Interest*, September 11 2022, accessed July 9, 2024, https://nationalinterest.org/print/feature/zawahiri's-assassination-proves-war-afghanistan-far-over-204691 .

43 See, e.g.: Haaretz, "How Hamas Attacked Israel: Minute-by-Minute," *Haaretz*, April 4, 2024, https://www.haaretz.com/israel-news/2024-04-18/ty-article-static/.premium/what-happened-on-oct-7/0000018e-c1b7-dc93-adce-eff753020000 . Notably, the Al Jazeera documentary "October 7" contains numerous inaccuracies, for instance, the claim that Hamas fighters received instructions at 6am and then gathered at assembly points; some may have, but video footage and other evidence reveals some Hamas fighters were already undertaking operations as part of the assault before 6am. This would also have been necessary for the rocket and missile barrage and launch of drones and paragliders recorded as in use not long after 6am. Also, the claim in the Al Jazeera documentary that no Hamas fighters knew the target before the operation is clearly false provided evidence of detailed planning that has been found (see below). Al Jazeera Investigations, "October 7" YouTube, March 20, 2024, accessed July 9, 2024, https://www.youtube.com/watch?v=_0atzea-mPY.

44 Noga Tarnopolsky and Shira Rubin, "Israel massed troops in the West Bank. Then Hamas attacked from Gaza," *Washington Post*, October 9, 2023, accessed July 9, 2024, https://www.washingtonpost.com/world/2023/10/09/israel-hamas-attack-gaza-intelligence/ .

45 Yaniv Kubovich, "The First Hours of the Israel-Hamas War: What Actually Happened?," *Haaretz*, October 17, 2023, accessed July 9, 2024, https://www.haaretz.com/haaretz-explains/2023-10-17/ty-article-magazine/.premium/the-first-hours-of-the-israel-hamas-war-what-actually-took-place/0000018b-38bc-d0ac-a39f-b9be58df0000 .

46 Patrick Kingsley, Aaron Boxerman and Gabby Sobelman, "'There Were Terrorists Inside': How Hamas's Attack on Israel Unfolded," *New York Times*, October 8, 2023, accessed July 9, 2024, https://www.nytimes.com/2023/10/08/world/middleeast/israel-hamas-attack.html

47 Alice Cuddy, "Hamas attack on Israel kibbutz Be'eri captured by mothers' WhatsApp group," *BBC,* October 13, 2023, accessed July 9, 2024, https://www.bbc.com/news/world-middle-east-67105618 .

48 Weininger, "'We knew what would happen': How Hamas attacked on October 7".

49 Claimed footage of this can be seen here: Joe Truzman @JoeTruzman, "I don't think I've watched so many rockets fired from one site in the Gaza Strip before," X formerly known as Twitter, December 8, 2023, accessed July 9, 2024, https://twitter.com/JoeTruzman/status/1732937352484700420 .

50 Washington Institute, "Weapon of Terror: Development and Impact of the Qassam Rocket," *Washington Institute*, Policy Watch 1352, March 11, 2008, accessed July 9, 2024, https://www.washingtoninstitute.org/policy-analysis/weapon-terror-development-and-impact-qassam-rocket .

51 Patrick Sullivan and John Amble, "What Happened To Iron Dome? A Lesson On The Limits Of Technology At War," *Modern War Institute at West Point*, October 10, 2023, accessed July 9, 2024, https://mwi.westpoint.edu/what-happened-to-iron-dome-a-lesson-on-the-limits-of-technology-at-war/ .

52 Divyam Sharma, "How Hamas Outfoxed Israel's Iron Dome, A Nearly Impenetrable Air Defence," *NDTV*, October 8, 2023, accessed July 9, 2024, https://www.ndtv.com/world-news/israel-palestine-hamas-gaza-iron-dome-how-israel-defends-its-skies-from-rocket-attacks-4460636 .

53 Mapping of the initial and later salvoes can be seen at: ACLED, "Fact Sheet: Israel and Palestine Conflict," *ACLED*, October 9, Updated October 31, 2023, https://acleddata.com/2023/10/10/fact-sheet-israel-and-palestine-conflict/ ; Wall Street Journal, "Israel at War With Hamas: Live Updates," *Wall Street Journal*, October 10, 2023, https://www.wsj.com/livecoverage/israel-hamas-gaza-rockets-attack-palestinians/card/map-where-hamas-militants-are-attacking-israel-UV8YHO8AqlUVIYzsyc6x ; Economist, "Hamas's attack was the bloodiest in Israel's history," *Economist*, October 12, 2023, https://www.economist.com/briefing/2023/10/12/hamass-attack-was-the-bloodiest-in-israels-history ; Lauren Leatherby, Karen Yourish and Elena Shao, "Maps: Tracking the Attacks in Israel and Gaza," *New York Times*, October 7, 2023, https://www.nytimes.com/interactive/2023/10/07/world/middleeast/israel-gaza-maps.html . All accessed July 9, 2024.

54 Swaine et al., "How Hamas exploited Israel's reliance on tech to breach barrier on Oct. 7."

55 Ibid.

[56] Patrick Kingsley and Ronen Bergman "The Secrets Hamas Knew About Israel's Military," *New York Times,* October 13, 2023, accessed July 9, 2024, https://www.nytimes.com/2023/10/13/world/middleeast/hamas-israel-attack-gaza.html .

[57] Peter Beaumont, "How did Hamas manage to carry out its rampage through southern Israel?," *Guardian*, October 9, 2023, accessed July 9, 2024, https://www.theguardian.com/world/2023/oct/09/how-did-hamas-manage-to-carry-out-its-rampage-through-southern-israel

[58] Beaule, "A detailed look at how Hamas secretly crossed into Israel."

[59] Ibid.

[60] Ibid.

[61] Ibid.

[62] Wall Street Journal, "Satellite Images Show Breaches of Gaza Border Wall at Erez Crossing," *Wall Street Journal*, October 10, 2023, accessed July 9, 2024, https://www.wsj.com/video/satellite-images-show-breaches-of-gaza-border-wall-at-erez-crossing/971C451E-C57D-4499-BC28-E84EC148D206 .

[63] Mezzofiore et al., "Videos show new details on how Hamas launched surprise assault on Israel."

[64] For a map of Hamas' main infiltration locations see: The Hindu, "The week in 5 charts," *The Hindu,* October 16, 2023, accessed July 9, 2024, https://images.app.goo.gl/NgmqBFLUaCgkWLAn7 .

[65] Granados, et al., "How Hamas breached Israel's 'Iron Wall'."

[66] For a compilation of Hamas clips of drones attacking Israeli observation towers see: Emanuel (Mannie) Fabian @manniefabian, X formerly known as Twitter, October 8, 2023, https://twitter.com/manniefabian/status/1710980029977424295. For detailed discussion of such attacks see, for example: Toler, "How Hamas Attacked Israel's Communications Towers." All accessed July 9, 2024.

[67] Toler, "How Hamas Attacked Israel's Communications Towers."

[68] Bergman and Kingsley, "How Israel's Feared Security Services Failed to Stop Hamas's Attack."

[69] Rubin and Morris, "How Hamas broke through Israel's border defenses during Oct. 7 attack."

[70] See, e.g.: Ibid.; Paul P. Murphy, "Video shows Hamas launching weaponized drone from Gaza during October 7 attack," *CNN*, October 29, 2023, accessed July 9, 2024, https://edition.cnn.com/middleeast/live-news/israel-hamas-war-gaza-news-10-30-23/h_ecd9b2b2a4b0a1199eebedfe3ce7562f .

[71] Rubin and Morris, "How Hamas broke through Israel's border defenses during Oct. 7 attack."

[72] Kaniewski, "Hamas: Learning about drone warfare from the war in Ukraine."

[73] Oakford et al., "Videos show how Hamas achieved its unprecedented surprise attack on Israel," *Washington Post*, 8 October, 2023, https://www.washingtonpost.com/world/2023/10/08/israel-gaza-videos-border/ ; Gianluca Mezzofiore, Paul P. Murphy and Allegra Goodwin, "Videos show new details on how Hamas launched surprise assault on Israel," *CNN*, October 8, 2023, https://edition.cnn.com/2023/10/08/middleeast/hamas-videos-visual-timeline/index.html . All accessed July 9, 2024.

[74] Hindustan Times, "Hamas Drone Drops Grenade On Israel's Flagship Merkava MK4 Tank; Watch What Happened Next," Hindustan Times, 21 October 21, 2023, https://www.hindustantimes.com/videos/world-news/hamas-drone-drops-grenade-on-israels-flagship-merkava-mk4-tank-watch-what-happened-next-101697864164906.html ; Younis Tirawi, يونس @ytirawi, X formerly known as Twitter, October 7, 2023, https://twitter.com/ytirawi/status/1710588898735251761. All accessed July 9, 2024.

[75] GeoConfirmed @GeoConfirmed, "GeoConfirmed ISR-PAL.," X formerly known as Twitter, October 7, 2023, https://twitter.com/GeoConfirmed/status/1710642285614977189 .

[76] See: DroneSec, "Hamas 7th October Intrusion Drones Observed," Version 1.4 *DroneSec*, 15. Access via: https://dronesec.com/white-paper/hamas-october-2023-intrusion-use-of-drones.

[77] Ibid.

[78] Although it is usually applied to state armed forces, there is an increasing tendency to apply it as a concept to non-state actors. It has been defined variously, see: Jonathan House, *Combined Arms Warfare in the Twentieth Century* (Kansas: Kansas University Press, 2001). Its essence is the use of various combat arms and weapons in concert to maximise overall efficacy and mitigate individual weaknesses. Combined arms are discussed in detail below. Notably, recently there has been a move by the US Army to expand what combined arms involves including civilian and cyber capabilities and for them to be used strategically, see: Gary Sheftick, "Army Operating Concept expands definition of combined arms," *U.S. Army*, October 20, 2014, accessed July 9, 2024, https://www.army.mil/article/136453/Army_Operating_Concept_expands_definition_of_combined_arms/ . Paradoxically, non-state actors may arguably be more adept at this expanded conception. Therefore, this alteration in the concept may serve to favour the perception of their capability, particularly regarding 'strategic' use and information operations, as well as cyber.

[79] Chávez and Swed, "How Hamas innovated with drones to operate like an army."

[80] Elisabeth Gosselin-Malo, "Hamas drones helped catch Israel off guard, experts say," *C4ISRNET*,

October 18, 2023; Joby Warrick, Ellen Nakashima, Shane Harris and Souad Mekhennet, “Hamas received weapons and training from Iran, officials say,” *Washington Post*, October 9 2023, https://www.washingtonpost.com/national-security/2023/10/09/iran-support-hamas-training-weapons-israel/. All accessed July 9, 2023

81 Soufan Center, “IntelBrief: Complex Attack by Hamas into Israel has Altered the Dynamics of the Conflict,” *Soufan Center Intel Brief*, October 9, 2023, accessed July 9, 2023, https://thesoufancenter.org/intelbrief-2023-october-9/ .

82 Kubovich, “The First Hours of the Israel-Hamas War: What Actually Happened?”

83 Ibid.

84 Octo7map, “Mapping the Massacre,” *Octo7map*, n.d., accessed July 9, 2024, https://oct7map.com .

85 This synchronisation or use “in concert” is noted for example by: Chávez and Swed, “How Hamas innovated with drones to operate like an army”; Gosselin-Malo, “Hamas drones helped catch Israel off guard, experts say”; David Hambling, “How Hamas Leveraged Cheap Rockets And Small Drones To Ambush Israel,” *Forbes*, October 9, 2023, https://www.forbes.com/sites/davidhambling/2023/10/09/how-hamas-leveraged-cheap-rockets-and-small-drones-to-ambush-israel/ ; Agnes Helou, How drone warfare in Israel could dramatically change if Hezbollah joins the fight: Analysts,” *Breaking* Defense, October 20, 2023, https://breakingdefense.com/2023/10/how-drone-warfare-in-israel-could-dramatically-change-if-hezbollah-joins-the-fight-analysts/. All accessed July 9, 2024.

86 Rubin and Morris, “How Hamas broke through Israel’s border defenses during Oct. 7 attack.”

87 Cuddy, “Hamas attack on Israel kibbutz Be’eri captured by mothers’ WhatsApp group.”

88 See, ibid.

89 Weininger, “‘We knew what would happen’: How Hamas attacked on October 7.”

90 Ibid.

91 CNN, “Hamas music festival attack investigation,” *CNN*, n.d., accessed July 9, 2024, https://edition.cnn.com/interactive/2023/10/middleeast/hamas-music-festival-attack-investigation-cmd-intl/ .

92 Cloud, et al., “Hamas Militants Had Detailed Maps of Israeli Towns, Military Bases and Infiltration Routes.”

93 Kubovich, “The First Hours of the Israel-Hamas War: What Actually Happened?”

94 Mezzofiore et al. “Videos show new details on how Hamas launched surprise assault on Israel.”

95 CNN, “Hamas video shows fighters storming Israel-Gaza border crossing,” *CNN*, October 7, 2023, accessed July 9, 2024, https://edition.cnn.com/videos/world/2023/10/07/hamas-fighters-storm-israel-gaza-border-crossing-sot-vpx-nr.cnn .

96 Barrons, “Israeli defence ministry footage of damaged Erez border crossing,” *Barrons*, October 17, 2023, https://www.barrons.com/video/israeli-defence-ministry-footage-of-damaged-erez-border-crossing/54B445C7-564C-4FF6-8E76-E13C5BE91552.html .

97 Roya TV, “Qassam Brigades publish summary of Sunday’s ‘Erez’ battle,” *Roya TV*, October 29, 2023, accessed July 9, 2024, https://en.royanews.tv/news/45878/2023-10-29 .

98 Hilo Glazer, “A Handful of Israeli Officers Saved 90 New Recruits From Hamas Terrorists. They Paid With Their Lives,” *Haaretz*, October 20, 2023, accessed July 9, 2024, https://www.haaretz.com/israel-news/2023-10-20/ty-article-magazine/.premium/a-few-idf-officers-saved-90-trainees-from-hamas-terrorists-they-paid-with-their-lives/0000018b-4da2-dc3c-a5df-ddaadf370000 .

99 Footage has since emerged of Hamas terrorists landing by boat on the beach proximate to Zikim. One boat reportedly managed to evade IDF, with the others reportedly being destroyed at sea. See, e.g., Emanuel Fabian, “New footage shows seaborne Hamas attack on October 7,” *Times of Israel*, December 2, 2023, accessed July 9, 2024, https://www.timesofisrael.com/liveblog_entry/new-footage-shows-seaborne-hamas-attack-on-october-7/ .

100 Mezzofiore et al. “Videos show new details on how Hamas launched surprise assault on Israel.”

101 David Horovitz, “The sole avenue of coexistence that became a Hamas killing field,” *Times of Israel*, November 23, 2023, accessed July 9, 2024, https://www.timesofisrael.com/the-sole-avenue-of-coexistence-that-became-a-hamas-killing-field/ .

102 Jeremy Diamond, “Exclusive footage of Hamas invading via paraglider,” *CNN*, October 25, 2023, accessed July 9, 2024, https://edition.cnn.com/videos/world/2023/10/25/exp-israel-gaza-attack-jeremy-diamond-war-fst-102512pseg1-cnni-world.cnn .

103 Horovitz, “The sole avenue of coexistence that became a Hamas killing field.”

104 ”ריקי לאירא לט ''ינושאר ולקתנש - רדגה דומצ בשומה ישנא לש תיאליעה הרובגה :הרשעה ביתנ לש חלודבה ליל,” *Israel Hayom*, October 12, 2023, accessed July 9, 2024, https://www.israelhayom.co.il/magazine/shishabat/article/14702377.

105 Ibid.

106 Bellingcat Investigation Team, “Geolocating Hamas-Led Attacks on Israeli Civilians,” *Bellingcat*, October 20, 2023, accessed July 9, 2024, https://www.bellingcat.com/news/2023/10/20/geolocating-hamas-led-attacks-on-israeli-civilians/ .

107 Casey Tolan, Audrey Ash, Isabelle Chapman and Curt Merrill, “Slain Hamas militants’ body camera videos show the preparation and tactics behind their terror attack on Israel,” *CNN*, October 26, 2023, accessed July 9, 2024, https://edition.cnn.com/interactive/2023/middleeast/hamas-attack-body-cam-videos-invs-dg/ .

108 Stewart Bell, “Investigation: The Hamas attack on an Israeli kibbutz, and how residents fought back,” *Global News*, October 24, 2023, accessed Juy 9, 2024, https://globalnews.ca/news/10042686/investigation-hamas-attack-an-israeli-kibbutz-residents-resist/ .

109 Efkar Lefkovitz, “Grandmother outsmarts Hamas terrorists in her home,” *Jewish News* Syndicate, October 9, 2023, accessed July 9, 2024, https://www.jns.org/grandmother-outsmarts-hamas-terrorists-in-her-home/ .

110 Rubin and Morris, “How Hamas broke through Israel’s border defenses during Oct. 7 attack.”

111 Nicky Hager, “Israel’s omniscient ears,” *Le Monde Diplomatique*, September 2010, accessed July 9, 2024, https://mondediplo.com/2010/09/04israelbase .

112 Bergman et al., “How Years of Israeli Failures on Hamas Led to a Devastating Attack.”

113 Al Mayadeen English, @MayadeenEnglish “#Watch Al-Qassam Brigades publishes footage of the Al-Zouari suicide drones,” X formerly known as Twitter, October 8, 2023, accessed July 9, 2024, https://twitter.com/MayadeenEnglish/status/1711008445808218158?s=20 .

114 Regarding the emergence of the Al-Zouari drone, see: Ansrollah, “Al-Qassam Brigades Announces ‘Zouari’ Aircraft Into Service,” *Ansaroollah*, May 19, 2019, https://www.ansarollah.com/archives/433646; United Against Nuclear Iran, “The Iranian Drone Threat,” *United Against Nuclear Iran*, Updated July 22, 33-39, esp. 33-34, https://www.unitedagainstnucleariran.com/The-iranian-drone-threat . All accessed July 9, 2024. Regarding the development of the Al-Zouari drone and the modified, loitering munition version the following details and sources provide important insights. Mohamed al-Zouari, a Tunisian-born engineer, was reportedly approached by Hamas in the early 2010s, to help them employ some of Hamas’ early drones. Hamas claims to have built the first reported Hamas drone model, the Ababeel1, overseen by Mohamed Al-Zouari. However, Jane’s considered it Iranian-built. Notably, a UN independent international Commission of inquiry asserts that Mohamed al-Zouari “supervised the use of the Ababeel 1” by Hamas and did not find that either he or Hamas built it. Furthermore, United Against Nuclear Iran, in their outstandingly detailed report on “The Iranian Drone Threat”, notes that the reconnaissance, attack/bombing capable, and loitering munition variants of the “Ababil-1… “are akin” to Iranian Ababil models. Thus, it is doubtful that Hamas built them from scratch, and it is almost certain that they were either supplied from Iran in large part or constructed using plans from Iran and parts. See: Ling, “The Dangerous Mystery of Hamas’ ‘Suicide Drones’”; Isabel Kershner and Lyons, Patrick J. Lyons, “Hamas Publishes Photo of a Drone It Says It Built,” *The New York Times*, July 14, 2014, https://www.nytimes.com/2014/07/15/world/middleeast/hamas-publishes-photo-of-a-drone-it-says-it-built.html?_r=0 ; Alon Ben-David, “Israel shoots down Hizbullah UAV,” *Jane’s Defence Weekly*, August 9, 2006, http://www.janes.com/defence/air_forces/news/jdw/jdw060810_1_n.shtml; United Nations, Report of the detailed findings of the independent international Commission of inquiry on the protests in the Occupied Palestinian Territory,” Human Rights Council, A/HRC/40/CRP.2, March 18, 2019, 118, fn 552, https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session40/Documents/A_HRC_40_74_CRP2.pdf ; United Against Nuclear Iran, “The Iranian Drone Threat”, 33-39, esp. 33-34, https://www.unitedagainstnucleariran.com/The-iranian-drone-threat . All accessed July 9, 2024.

115 See: Page, “Loitering Munitions and Drones: The Urgent Need for Clarity.”

116 Samuel Bendett,@sambendett “4/ Apparently, Hamas drones posted above in the first video,” X formerly known as Twitter, October 8, 2023, accessed July 9, 2024, https://twitter.com/sambendett/status/1711004280654635512 .

117 Jake Godin @JakeGodin, “Hamas video from earlier showing the group launching Zouari drones,” X formerly known as Twitter, October 8, 2023, accessed July 9, 2024, https://twitter.com/JakeGodin/status/1711010634190430575 .

118 Justin Ling, “The Dangerous Mystery of Hamas’ ‘Suicide Drones’,” *WIRED*, October 21, 2023, accessed July 9, 2024, https://www.wired.com/story/hamas-drones-israel-war/ .

119 The littoral is the space between where ground forces and bombers, MALE drones, and unmanned aerial systems (UAS) operate, which loitering munitions often use. See: Maximilian K. Bremer & Kelly A. Grieco, “The Air Littoral- Another Look,” Parameters 51, no. 4 (2021), 67-80, DOI:10.55540/0031-1723.3092. Watling and Kaushal term this the “seam”. Jack Watling and Sidharth Kaushal, “The Democratisation of Precision Strike in the Nagorno-Karabakh Conflict,” *Royal United Services Institute*, Commentary, 22 October 2020, accessed July 9, 2024, https://rusi.org/explore-our-research/publications/commentary/democratisation-precision-strike-nagorno-karabakh-conflict .

[120] Hambling, "How Hamas Leveraged Cheap Rockets And Small Drones To Ambush Israel."

[121] Greg Waldron, "Drones, paragliders featured in Hamas attack against Israel," *Flight Global*, October 10, 2023, accessed July 9, 2024, https://www.flightglobal.com/defence/drones-paragliders-featured-in-hamas-attack-against-israel/155301.article .

[122] IRNA, "Palestine's al-Qassam Brigades unveils new drone," *IRNA*, October 8, 2023, accessed July 9, 2024, https://en.irna.ir/news/85251878/Palestine-s-al-Qassam-Brigades-unveils-new-drone .

[123] Times of Israel, "IDF says drone launch positions on residential roofs destroyed," *Times of Israel*, October 13, 2023, https://www.timesofisrael.com/liveblog_entry/idf-says-drone-launch-positions-on-residential-roofs-destroyed/ ; DroneSec, "Hamas 7th October Intrusion Drones Observed." All accessed July 9, 2024.

[124] Mayan Jaffe-Hoffman, "WATCH: IDF assassinates head of Hamas aerial array," *Jerusalem Post*, November 28, 2023, accessed July 9, 2023, https://www.jpost.com/breaking-news/article-770541 .

[125] Samuel Bendett @sambendett "5/ Hamas recently published a video of some kind of command and control center for their UAV and drone operations over Israel," X formerly known as Twitter, October 9, 2023, accessed July 9, 2024, https://twitter.com/sambendett/status/1711421272561725935 .

[126] See, e.g.: Jeffrey A. Edmonds and Samuel Bendett, "Russia's Use of Uncrewed Systems in Ukraine", *CNAS*, March 2023, accessed July 9, 2024, https://www.cna.org/reports/2023/05/russias-use-of-drones-in-ukraine .

[127] Rassler, "Remotely Piloted Innovation Terrorism, Drones and Supportive Technology," 30-31. Also see: Veilleux-Lepage and Archambault, "A Comparative Study of Non-State Violent Drone use in the Middle East," *International Centre for Counter-Terrorism ICCT*, July 9, 2022, 29-32. Accessed July 9, 2024, https://www.icct.nl/publication/comparative-study-non-state-violent-drone-use-middle-east ; United Against Nuclear Iran, " Iranian Drone Threat" ; Lenny Ben-David, "Hamas' Advanced Weaponry: Rockets, Artillery, Drones, Cyber," *Jerusalem Center for Public Affairs,* August 1, 2021, https://jcpa.org/article/hamas-advanced-weaponry-rockets-artillery-drones-cyber/.

[128] Regarding Iranian support to Hamas for the 7 October attack, see, e.g., Joby Warrick, et al. "Hamas received weapons and training from Iran, officials say." Notably, considerable debate exists about the extent of Iran's involvement in the 7 October attack. For a helpful summary of a variety of views see: Jim Zanotti, Jeremy M. Sharp, and Christopher M. Blanchard, "Israel and Hamas October 2023 Conflict: Frequently Asked Questions," *Congressional Research Service*, Report R47754, October 20, 2023, 18-19, https://crsreports.congress.gov/product/pdf/R/R47754 . More recently, see: Phillip Smyth, "The Path to October 7: How Iran Built Up and Managed a Palestinian 'Axis of Resistance'," *CTC Sentinel*, 16 no. 11, December 2023, 25-40; MEMRI, "Iranian Officials Acknowledge Iran's Role In Planning And Executing October 7 Hamas Invasion And Massacres In Southern Israel ," *Middle East Media Research Institute*, Special Dispatch No. 11439, July 10, 2024, https://www.memri.org/reports/iranian-officials-acknowledge-irans-role-planning-and-executing-october-7-hamas-invasion-and .More generally regarding Iran's drone programme and its support to non-state actors, see: Golnaz Esfandiari, "Iran Deploys Drones To Target Internal Threats, Protect External Interests," *Radio Free Europe / Radio Liberty*, January 18, 2022, https://www.rferl.org/a/iran-drone-program-threats-interests/31660048.html. All accessed July 9, 2024.

[129] For an excellent source of states with drone programmes and the date of this, in addition to other data, see: Peter Bergen, David Sterman, Melissa Salyk-Virk, Christopher Mellon, Alyssa Sims, and Albert Ford, "World of Drones: Examining the Proliferation, Development, and Use of Armed Drones," *New America Foundation*, last updated 2020, accessed July 9, 2024, https://www.newamerica.org/future-security/reports/world-drones/who-has-what-countries-with-armed-drones .

[130] See: Alex Fishman "The New Explosive Drone Threat from Gaza," *Ynetnews*, July 29, 2018, accessed July 9, 2024, https:// www.ynetnews.com/articles/0,7340,L-5318598,00.html ; Veilleux-Lepage and Archambault, "A Comparative Study of Non- State Violent Drone use in the Middle East,", 31 .

[131] See, e.g.: Ling, "The Dangerous Mystery of Hamas' Missing 'Suicide Drones'."

[132] See: Rassler, "Remotely Piloted Innovation," 31.

[133] Ibid., 33.

[134] Veilleux-Lepage and Archambault, "A Comparative Study of Non- State Violent Drone use in the Middle East," 29-32.

[135] See: Rassler, "Remotely Piloted Innovation," 30,31; Ling, "The Dangerous Mystery of Hamas' Missing 'Suicide Drones'."

[136] See, for eg: Joseph Trevthick, "Largest Rocket Barrage From Gaza Ever Hits Central Israel Amid Fears Of An Imminent War," *Drive*, May 11, 202,1 https://www.thedrive.com/the-war-zone/40561/largest-rocket-barrage-from-gaza-ever-hits-central-israel-amid-fears-of-an-imminent-war ; Joseph Trevthick, "Palestinian Militants Are Now Launching Suicide Drones At Israel," *Drive*, May 13, 2021,

https://www.thedrive.com/the-war-zone/40601/palestinian-militants-are-now-launching-suicide-drones-at-israel ; Lawahez Jabari, Paul Goldman, Rachel Elbaum and Yuliya Talmazan, "Hamas fires rockets into Israel as tensions in Jerusalem boil over," *NBC*, May 10, 2021, https://www.nbcnews.com/news/world/hundreds-injured-palestinians-israeli-forces-clash-holy-site-jerusalem-n1266812l . All accessed July 9, 2024.

137 See, e.g.: David S. Cloud, Anat Peled and Dov Lieber, "Hamas Militants Had Detailed Maps of Israeli Towns, Military Bases and Infiltration Routes," *Wall Street Journal,* October 12, 2023, accessed July 9, 2024, https://www.wsj.com/world/middle-east/hamas-militants-had-detailed-maps-of-israeli-towns-military-bases-and-infiltration-routes-7fa62b05 .

138 See: Smyth, "The Path to October 7"; MEMRI, "Iranian Officials Acknowledge Iran's Role In Planning And Executing October 7 Hamas Invasion And Massacres In Southern Israel ."

139 Gabrielle Weininger, "'We knew what would happen': how Hamas attacked on October 7," *The Sunday Times*, November 10, 2023, accessed July 9, 2024, https://www.thetimes.co.uk/article/we-knew-what-would-happen-how-hamas-attacked-on-october-7-63dd3c8cx .

140 Yani Kubovich, "The Women Soldiers Who Warned of a Pending Hamas Attack – and Were Ignored," *Haaretz*, November 20, 2023, accessed July 9, 2024, https://www.haaretz.com/israel-news/2023-11-20/ty-article-magazine/.premium/the-women-soldiers-who-warned-of-a-pending-hamas-attack-and-were-ignored/0000018b-ed76-d4f0-affb-eff740150000 .

141 Cloud et al., "Hamas Militants Had Detailed Maps of Israeli Towns, Military Bases and Infiltration Routes."

142 Jerusalem Post Staff, "IDF commanders ignored lookouts' warnings over Hamas massacre - report," *Jerusalem* Post, November 19, 2023, accessed July 9, 2024, https://www.jpost.com/israel-news/article-773974 .

143 Times of Israel, "TV report: Hamas downed IDF drones and a surveillance camera weeks before Oct. 7," *Times of Israel*, November 5, 2023, accessed July 9, 2024, https://www.timesofisrael.com/liveblog_entry/tv-report-hamas-downed-idf-drones-and-a-surveillance-camera-weeks-before-oct-7/ .

144 BBC, "Egypt warned Israel days before Hamas struck, US committee chairman says," *BBC,* October 12, 2023, accessed July 2024, https://www.bbc.com/news/world-middle-east-67082047 .

145Ronen Bergman, Mark Mazzetti and Maria Abi-Habib, "How Years of Israeli Failures on Hamas Led to a Devastating Attack," *New York Times*, October 29, 2023, accessed July 9, 2024, https://www.nytimes.com/2023/10/29/world/middleeast/israel-intelligence-hamas-attack.html .

146 Jerusalem Post Staff, "IDF commanders ignored lookouts' warnings over Hamas massacre - report."

147 Times of Israel, "TV report: Hamas downed IDF drones and a surveillance camera weeks before Oct. 7."

148 Rubin and Morris, "How Hamas broke through Israel's border defenses during Oct. 7 attack."

149 Yani Kubovich, "Despite Repeated Warnings, Israeli Army Neglected Malfunctioning Observation Balloons on Gaza Border," *Haaretz*, October 23, 2023, accessed July 9, 2024, https://www.haaretz.com/israel-news/2023-10-23/ty-article/.premium/despite-warnings-idf-neglected-malfunctioning-observation-balloons-on-gaza-border/0000018b-5b84-d8e2-a1eb-fb96f45b0000 .

150 Jerusalem Post Staff, "IDF commanders ignored lookouts' warnings over Hamas massacre - report."

151 Ibid.

152 Regarding these tunnel systems and their proximity to the border with Israel, see, for example: a Fitch and Rory Jones, "Map Shows Labyrinth of Tunnels Made by Hamas Under Gaza Identified by Israel," *Wall Street Journal*, October 29, 2023, accessed July 9, 2024, https://www.wsj.com/livecoverage/israel-hamas-war-biden/card/map-shows-labyrinth-of-tunnels-made-by-hamas-under-gaza-identified-by-israel-IieNDixn5Bs78HeUi46v .

153 See: Noga Tarnopolsky and Shira Rubin, "Israel massed troops in the West Bank. Then Hamas attacked from Gaza," *Washington Post*, October 9, 2023, https://www.washingtonpost.com/world/2023/10/09/israel-hamas-attack-gaza-intelligence/ ; Emanuel Fabian, "2 commando companies said diverted from Gaza border to West Bank days before Oct. 7," *Times of Israel,* December 5, 2023, https://www.timesofisrael.com/2-commando-companies-said-diverted-from-gaza-border-to-west-bank-days-before-oct-7/ . All accessed July 9, 2024.

154See: Daniella Cheslow, "Israel and the West reckon with a high-tech failure," *Politico*, October 10, 2023, accessed July 9, 2024, https://www.politico.com/news/2023/10/10/israel-hamas-technology-failure-00120667.

155 See, e.g.: John Ismay @johnismay, "These videos from Gaza showed a type of small improvised munition," X formerly known as Twitter, October 11, 2023, accessed July 9, 2024, https://twitter.com/johnismay/status/1712109301760708719 .

156 Chávez and Swed, "How Hamas innovated with drones to operate like an army."

157 Ben Watson, "The Drones of ISIS," *Defense One*, January 12, 2017, accessed July 9, 2024,

https://www.defenseone.com/technology/2017/01/drones-isis/134542/ .

158 Alessandra Scotto Di Santolo, "Ukrainian special forces destroy key Russian observation tower in blow to Putin," *Daily Express*, March 6, 2023, accessed July 9, 2024, https://www.express.co.uk/news/world/1742864/ukraine-kraken-russia-tower-Bryansk-Oblast-kamikaze-drone .

159 Antebi and Yanko-Avikasis, "Life and Death in the Hands of the Drone: The Small, Cheap Devices Early in the Swords of Iron War."

160 Marissa Newman, "Hamas's Cheap, Makeshift Drones Are Outsmarting Israel's High-Tech Military," *Bloomberg*, December 19, 2023, accessed July 9, 2024, https://www.bloomberg.com/news/articles/2023-12-19/israel-s-advanced-defenses-are-pierced-by-makeshift-hamas-drones-in-gaza-war .

161 For example, by ISIS to disable recording and geofencing, see: Veilleux-Lepage and Archambault, "A Comparative Study of Non- State Violent Drone use in the Middle East," 62.

162 See: Patrick Tucker, "The next drone war is coming to Gaza," *Defense One*, October 17, 2023, accessed July 9, 2024, https://www.defenseone.com/technology/2023/10/next-drone-war-coming-gaza/391277/ .

163 Those publications that have noted the coordinated and combined use of drones with other actions include: Elisabeth Gosselin-Malo, "Hamas drones helped catch Israel off guard, experts say," *C4ISRNET,* October 18, 2023, https://www.c4isrnet.com/global/mideast-africa/2023/10/18/hamas-drones-helped-catch-israel-off-guard-experts-say/ ; with relatively more detail: Chávez and Swed, "How Hamas innovated with drones to operate like an army," *Bulletin of the Atomic Scientists*, November 1, 2023, https://thebulletin.org/2023/11/how-hamas-innovated-with-drones-to-operate-like-an-army/ . All accessed July 9, 2024.

164 Chávez and Swed, "How Hamas innovated with drones to operate like an army."

165 See: Maurer, "ISIS's Warfare Functions" 229.

166Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton, Princeton University Press, 2004), accessed July 9, 2024, https://press.princeton.edu/books/paperback/9780691128023/military-power .

167 Jonathan M. House, "Toward Combined Arms Warfare: A Survey of 20th~Century Tactics, Doctrine, and Organization," *Combat Studies Institute*, Research Survey no. 2, August 1984, accessed July 9, 2024, https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/house.pdf .

168 Gilbert wrote: "We have gotten into the fashion of talking of cavalry tactics, artillery tactics, and infantry tactics. This distinction is nothing but mere abstraction. There is but one art, and that is the tactics of the combined arms. The tactics of a body of mounted troops composed of the three arms is subject to the same established principles as is that of a mixed force in which foot soldiers bulk largely. The only difference is one of mobility." Gerald E.L. Gilbert, *The Evolution of Tactics* (London, 1907), 183-4. Major Gerald E. L. Gilbert was an officer in the British Indian Army and wrote this work while on duty in India. Notably, he was decorated in August 1908 in recognition of his services in connection with operations against the Zakka Khel and Mohmand tribes (that inhabit Afghanistan and now what is part of Pakistan) in July 1908, i.e. non—state actors. See: https://www.thegazette.co.uk/London/issue/28168/supplement/6066/data.pdf

169 Biddle, *Military Power*, 38.

170 See, for example: Michael Evans and Alan Ryan (eds), "From Breitenfeld to Baghdad Perspectives on Combined Arms Warfare," Land Warfare Studies Centre Working Paper, no. 122, July 2003, accessed July 9, 2024, https://researchcentre.army.gov.au/sites/default/files/wp122-from_breitenfeld_to_baghdad_michael_evans_alan_ryan.pdf .

171 William S. Lind, *Maneuver Warfare Handbook* (New York: Routledge, 1985); House, "Toward Combined Arms Warfare"; House, *Combined Arms Warfare in the Twentieth Century*; Biddle, *Military Power*, 37-39.

172 Lind, *Maneuver Warfare Handbook*, 12.

173 Sheftick, "Army Operating Concept expands definition of combined arms."

174 Ervin J. Rokke, Thomas A. Drohan, and Terry C. Pierce, "Combined Effects Power," *Joint Force Quarterly* 73 (2nd Quarter, April 2014), https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-73/Article/577501/combined-effects-power/ ; Sheftick, "Army Operating Concept expands definition of combined arms." All accessed July 9, 2024.

175 Benjamin Jensen and Matthew Strohmeyer, "The Changing Character of Combined Arms," *War on the Rocks*, May 23, 2022, accessed July 9, 2024, https://warontherocks.com/2022/05/the-changing-character-of-combined-arms/ .

176 Maurer, "ISIS's Warfare Functions: A Systematized Review of a Proto-state's Conventional Conduct of Combat Operations," 232.

177 Ibid., 233.

[178] Austin C. Doctor and James I. Walsh, "The Coercive Logic of Militant Drone Use," *Parameters*, 51, no. 2 (Summer 2021), 73-84, 81, doi:10.55540/0031-1723.3069. A similar argument is made by them in: Austin C. Doctor and James I. Walsh, "The Militant Drone Playbook," *War on the Rocks,* August 12, 2021, https://warontherocks.com/2021/08/the-militant-drone-playbook/ ; Robert A. Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca, NY: Cornell University Press, 1997). All accessed September 20, 2024.

[179] Chávez and Swed, "How Hamas innovated with drones to operate like an army."

[180] See, e.g.: Daniela Pistoia, "Detecting and Neutralizing Mini-Drones: Sensors and Effectors against an Asymmetric Threat," *Journal of the JAPCC*, 25, 81-87; Ulzhalgas Seidaliyeva,Lyazzat Ilipbayeva, Kyrmyzy Taissariyeva, Nurzhigit Smailov, and Eric T. Matson, "Advances and Challenges in Drone Detection and Classification Techniques: A State-of-the-Art Review," *Sensors* 24, no. 125 (2024), https://doi.org/10.3390/s24010125 .

[181] Horovitz, "The sole avenue of coexistence that became a Hamas killing field."

[182] See: DroneSec, "Hamas 7th October Intrusion Drones Observed."

[183] Where the actions an adversary takes to defend themselves from one of two or more arms used in sequence against them defends against the other arms. Lind, *Maneuver Warfare Handbook*.

[184] Horovitz, "The sole avenue of coexistence that became a Hamas killing field."

[185] Dr Lirab Antebi, a Research Fellow at the Institute for National Security Studies, has observed parallels with the 1987's "Night of the Gliders", (see: Jonathan Edwards, "Paragliding fighters flew into Israel. A similar attack happened 35 years ago," *Washington Post*, October 9, 2023, https://www.washingtonpost.com/history/2023/10/09/israel-night-of-the-gliders-2023/). This was when a member of the Popular Front for the Liberation of Palestine (PFLP) terrorist group used a glider to infiltrate Israel from southern Lebanon and killed six soldiers (see: Oded Yaron, "Hamas Drone Assault Surprised Israel, Using Russia-Ukraine War Tactics," *Haaretz*, October 9, 2023, https://www.haaretz.com/israel-news/security-aviation/2023-10-09/ty-article/.premium/hamas-drone-assault-surprised-israel-using-russia-ukraine-war-tactics/0000018b-155d-d2fc-a59f-d55d05eb0000 ). Notably, October 7, 2023, is not the first time Hamas has used motorised paragliders; it did so in 2003 (see: Zohar Blumenkrantz, "New Anti-air Terror Measures: IDs for Powered Paragliders," *Haaretz,* January 1, 2003, https://www.haaretz.com/2003-01-01/ty-article/new-anti-air-terror-measures-ids-for-powered-paragliders/0000017f-df33-db5a-a57f-df7bbef60000 ), and it has been planning such attacks for some time (Advi Sterman, "Captured Hamas operative reveals paragliding attack plan," *Times of Israel*, July 30, 2014, https://www.timesofisrael.com/captured-hamas-operative-reveals-paraggliding-attack-plan/ ). All accessed July 9, 2024.

[186] Benjamin Jensen and Matthew Strohmeyer, "The Changing Character of Combined Arms," *War on the Rocks*, May 23, 2022, accessed July 9, 2024, https://warontherocks.com/2022/05/the-changing-character-of-combined-arms/ .

[187] Since the October 7, it has emerged that both the IDF and Israeli political leadership were confident border-wall defences and deterrence worked robustly against Hamas and Palestinian Islamic Jihad (PIJ) (see: Ronen Bergman, Patrick Kingsley, "How Israel's Feared Security Services Failed to Stop Hamas's Attack," *New York Times*, October 10, 2023, https://www.nytimes.com/2023/10/10/world/middleeast/israel-gaza-security-failure.html; Samuel Granados, Ruby Mellen, Lauren Tierney, Artur Galocha, Cate Brown and Aaron Steckelberg "How Hamas breached Israel's 'Iron Wall'," *The Washington Post*, October 10, 2023, https://www.washingtonpost.com/world/2023/10/10/how-hamas-entered-israel/ ; Mehul Srivastava "Israeli intelligence 'dismissed' detailed warning of Hamas raid," *Financial Times*, November 24, 2023, https://www.ft.com/content/277573ae-fbbc-4396-8faf-64b73ab8ed0a ). So much so, that large attacks against Israel were regarded by influential sections of Israel's political and military leadership as not remotely likely, which proved deeply mistaken (Antonio Pita, "Why powerful Israel did not see the Hamas attack coming," *El Pais*, October 9, 2023, https://english.elpais.com/international/2023-10-09/why-powerful-israel-did-not-see-the-hamas-attack-coming.html). Much store had been set in deterrence and high-tech solutions including sensors, remote control cameras, and telecommunications, coupled with fixed positions and walls, with minimal personnel (David H. Freedman, "Israel's High-Tech Border Failure Could Happen in the U.S., Experts Say," *Newsweek*, 15 November 2023, https://www.newsweek.com/2023/11/24/israels-high-tech-border-failure-could-happen-us-experts-say-1843772.html). This occurred as part of the IDF's 2015 strategy, the first ever to be published and made publicly available, and latterly its operational concept of "Decisive Victory", initiated in 2020. The IDF's 2015 strategy has been translated into English by the Belfer Center, Harvard University. Notable emphasis on technology and deterrence can be seen throughout it as can a less aggressive posture that this in part entails. See: Belfer Center, "Deterring Terror How Israel Confronts the Next Generation of Threats," Transl. Susan Rosenberg, *Belfer Center for International Affairs, Harvard University,* 2016, https://www.belfercenter.org/sites/default/files/files/publication/IDF%20doctrine%20translation%20-%20web%20final2.pdf . Regarding "Decisive Victory", see, e.g.: Jean-Loup Samaan, "'Decisive Victory' and Israel's Quest For a New Military Strategy," *Middle East Policy* 30, no. 30 (Autumn (Fall) 2023), 3–15,

https://doi.org/10.1111/mepo.12701. All accessed July 9, 2024.

188 Both foundational documents placed a heavy emphasis on technological solutions to ISR, and precision strike, and by incorporating smaller and more manoeuvrable units, as well as the extensive use of air power (including drones) for ISR, target acquisition, and with which to conduct strikes. A good overview is provided by Franz-Stefan Gady, however, the IDF's proclivity for the use of high-tech solutions and an increased emphasis on deterrence rather than a more aggressive stance against Hamas and other groups that it saw were becoming increasingly technologically capable pre-dates the 2020 "Decisive Victory" operating concept. Franz-Stefan Gady, "Israel's Military Tech Fetish Is a Failed Strategy," *Foreign Policy*, October 26, 2023, https://foreignpolicy.com/2023/10/26/israel-hamas-gaza-military-idf-technology-surveillance-fence-strategy-ground-war/. By October 7, elements of "Decisive Victory" were being tested – although it had not been fully implemented partly because of delays in the five-year military reform package (named the *Tnufa* program) initiated in 2020 - see: Shmuel Even, "The "Tnufa" Multi-Year Plan for the IDF: Where are the Cabinet Approval and the Budgets?," *INSS*, Insight No. 1357, August 5, 2020, https://www.inss.org.il/publication/tnufa-where-is-the-cabinet/. This includes for example with: enhanced technology to monitor the border including the use of cameras and remote-controlled weapons; the implementation and use of increasingly sophisticated communications; and the formation and integration of elite mobile units such as the "Ghost" special forces (officially Unit 888 "*Refaim*"). See: Anna Ahronheim, "IDF's Ghost multi-dimensional unit completes first drill," *Jerusalem Post*, July 24, 2020, https://www.jpost.com/israel-news/idfs-ghost-multi-dimensional-unit-completes-first-drill-636102 ; Citizen Frank, "Respected Leader of Israel 'Ghost' Commando Unit Killed Fighting Hamas," CF, October 8, 2023, https://www.cf.org/news/respected-leader-of-israel-ghost-commando-unit-killed-fighting-hamas/ . All accessed July 9, 2024.

189 Regarding the Ghost forces, their commander was killed on October 7, see, e.g.: Alia Shoaib, "2 of Israel's elite commanders and many officers have been killed in the Hamas war launched from Gaza: says IDF," *Business Insider*, October 8, 2023, accessed July 9, 2024, https://www.businessinsider.com/israels-best-commanders-many-officers-killed-hamas-war-gaza-idf-2023-10?op=1 .

190 Hoffmann, "Understanding Hamas's Genocidal Ideology."

191 Jonathan Marcus, "Combat drones: We are in a new era of warfare - here's why," *BBC*, February 4, 2022, accessed July 9, 2024, https://www.bbc.com/news/world-60047328 .

192 Boyle, *The Drone Age*; Arthur Holland Michel, "Biplanes, Satellites, and Drones: A High Resolution History of Eyes in the Sky," *Oxford Research Encyclopaedia of Criminology*, July 27, 2017, https://oxfordre.com/criminology/view/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-127; Ann Rogers and John Hill, *Unmanned: Drone Warfare and Global Security* (London: Pluto Press, 2014). All accessed July 9, 2024.

193 Early concern regarding this was expressed by, e.g.: Michael A. Gips, "A Remote Threat," *Security Management*, October 2002, www.securitymanagement.com . Gips notes that one security expert, a former intelligence officer, Louis Mizell, has recorded 43 cases involving 14 terrorist groups in which remote-control delivery systems were "either threatened, developed, or actually utilized." Also see: Robert J. Bunker, "Terrorist and insurgent unmanned aerial vehicles: use, potentials, and military implications," (Carlisle, PA: US Army War College Press, 2015); Larry Friese with N.R. Jenzen-Jones & Michael Smallwood, "Emerging Unmanned Threats: The use of commercially-available UAVs by armed non-state actors," Armed Research Services (ARES) Special Report No. 2, Perth Australia, 2016 ; Steven Stalinsky and R. Sosnow, "A Decade of Jihadi Organizations' Use of Drones: From Early Experiments by Hizbullah, Hamas, And Al-Qaeda To Emerging National Security Crisis For The West As ISIS Launches First Attack Drones," *Middle East Media Research Institute*, February 21, 2017, https://www.memri.org/reports/decade-jihadi-organizations-use-drones-–-early-experiments-hizbullah-hamas-and-al-qaeda*.* All accessed July 9 2024.

194 Antebi and Yanko-Avikasis, "Life and Death in the Hands of the Drone: The Small, Cheap Devices Early in the Swords of Iron War."

195 See: Gabriel Levin, "Gaza's Past and Present Explained," *Voice of America*, October 15, 2023, https://www.voanews.com/a/gaza-past-and-present-explained/7306915.html ; Wilson Center, "Doctrine of Hamas," *Wilson Center*, October 20, 2023, https://www.wilsoncenter.org/article/doctrine-hamas . All accessed July 9, 2024.

196 Antebi and Yanko-Avikasis, "Life and Death in the Hands of the Drone: The Small, Cheap Devices Early in the Swords of Iron War."

197 See, e.g.: Simon Scarr, Adolfo Arranz, Jonathan Saul, Han Huang, Jitesh Chowdhury and Vijdan Mohammad Kawoosa, "Red Sea attacks," *Reuters*, February 2, Updated March 8, 2024, accessed July 9, 2024, https://www.reuters.com/graphics/ISRAEL-PALESTINIANS/SHIPPING-ARMS/lgvdnngeyvo/ .

198 See: Rassler, "Remotely Piloted Innovation Terrorism, Drones and Supportive Technology," 30-31; Veilleux-Lepage and Archambault, "A Comparative Study of Non- State Violent Drone use in the Middle East," 29-32.

199 Alastair MacDonald, "The Race to Defend Against Drone Warfare Plays Out in Ukraine," *Wall Street Journal*, December 15, 2023, accessed July 9, 2024, https://www.wsj.com/world/the-race-to-defend-against-drone-warfare-plays-out-in-ukraine-96335409 .

200 See:Newman, "Hamas's Cheap, Makeshift Drones Are Outsmarting Israel's High-Tech Military."

201 Regarding Iran's crucial role for the development of Hamas' drone capability see, e.g: Rassler, "Remotely Piloted Innovation Terrorism, Drones and Supportive Technology," 30-31; Arthur Holland Michel and Dan Gettinger, "A Brief History of Hamas and Hezbollah's Drones," Bard Center for the Study of the Drone, July 14, 2014, https://dronecenter.bard.edu/hezbollah-hamas-drones/ ;Veilleux-Lepage and Archambault, "A Comparative Study of Non- State Violent Drone use in the Middle East," 29-32. United Against Nuclear Iran, "The Iranian Drone Threat," 33-39, is particularly detailed. Regarding the question of Iran's more recent support to Hamas for its drone and loitering munition capability, see: Nissenbaum et al., "With Iranian Help, Hamas Builds 'Made in Gaza' Rockets and Drones to Target Israel"; Yaakov Lappin, "Hamas's UAV fleet bears the fingerprints of Iran," *Jewish News Syndicate*, September 12, 2023, https://www.jns.org/israel-palestinianconflict/hamas/23/9/12/318080/ . Also see: All accessed July 9, 2024.

202 Brown et al., "How the Army Out-Innovated The Islamic State's Drones."

203 See: Vikram Mittal, "The Challenges Of Counter-Drone Technology As Seen In Recent Conflicts," *Forbes,* October 18, 2023, accessed September 20, 2024 , https://www.forbes.com/sites/vikrammittal/2023/10/18/the-challenges-of-counter-drone-technology-as-seen-in-recent-conflicts/ . Notably, in an important scholarly article Calcara et al., cast doubt on drones' ability to evade air defences, however, their focus was on MALE or medium altitude, long endurance drones; these are much larger than many of the small drones used by Hamas in the October 7 attack. See: Calcara et al., "Will the Drone Always Get through?"

204 Antebi and Yanko-Avikasis, "Life and Death in the Hands of the Drone: The Small, Cheap Devices Early in the Swords of Iron War."

205 See, e.g.: Mittal, "The Challenges Of Counter-Drone Technology As Seen In Recent Conflicts."

206 Liran Antebi and Matan Yanko-Avikasis make this point well: "in at least two reports by Israel's State Comptroller, which argued that Israel is not sufficiently prepared to deal with this threat", Antebi and Yanko-Avikasis, "Life and Death in the Hands of the Drone: The Small, Cheap Devices Early in the Swords of Iron War."

PT PERSPECTIVES ON TERRORISM

Research Article

# More is More: Scaling up Online Extremism and Terrorism Research with Computer Vision

Stephane J. Baele,* Lewys Brace, and Elahe Naserian

Volume XIX, Issue 1
March 2025

ISSN: 2334-3745
DOI: 10.19165/2025.1559

**Abstract:** Scholars and practitioners investigating extremist and violent political actors' online communications face increasingly large information environments containing ever-growing amounts of data to find, collect, organise, and analyse. In this context, this article encourages terrorism and extremism analysts to use computational visual methods, mirroring for images what is now routinely done for text. Specifically, we chart how computer vision methods can be successfully applied to strengthen the study of extremist and violent political actors' online ecosystems. Deploying two such methods – unsupervised deep clustering and supervised object identification – on an illustrative case (an original corpus containing thousands of images collected from incel platforms) allows us to explain the logic of these tools, to identify their specific advantages (and limitations), and to subsequently propose a research workflow associating computational methods with the other visual analysis approaches traditionally leveraged.

** Corresponding Author: Stephane J. Baele, University of Louvain. E-mail: stephane.baele@uclouvain.be*

# Introduction

Technological advances, such as the growth of the internet and its evolution towards web 2.0, increasingly powerful computer hardware, the development of user-friendly software interfaces, and now AI-powered tools, have significantly changed our socio-political landscape. Extremism and political violence are no exception: movements from across the world and the ideological spectrum have a history of adapting to technological innovation and embracing the newest IT technologies to better organise, finance themselves, and communicate.[1] The spectacular growth of the far-right online ecosystem[2] or the deployment by ISIS of a "full-spectrum propaganda"[3] are the two most visible examples of radical political actors taking full advantage of digital tools to proselytise and recruit, build support communities, polarise target societies, and intimidate purported enemies.

This evolution is synonymous with escalating amounts of extremist content being circulated online. Berger and Morgan, for example, estimated there to be 46,000 accounts supporting ISIS on Twitter between September and December 2014, amounting to millions of messages –[4] with Twitter being only one piece of ISIS's vast propaganda jigsaw, alongside its newspaper, magazines, videos, books, songs, and many more. Likewise, Horta-Ribeiro and colleagues' exploration of the "manosphere" gathered no less than 28 million posts from more than 50 misogynistic online communities (which is only a segment of the full environment).[5] In other words, sprawling "e-extremism"[6] generates enormous quantities of (meta-)data.

The sheer scale of this content has naturally pushed scholars to use computer-assisted methods geared at the localisation, collection, and analysis of large corpora and associated datasets, gaining a type of macro-level knowledge that granular qualitative studies could never hope to reach. Increased computational power has made investigations of extremely large and multidimensional datasets technically possible. As Grimmer, Roberts, and Stewart rightly observed (for political studies in general), while "for much of its history, empirical work in the social sciences has been defined by scarcity, […] social scientists are now in an era of data abundance",[7] a statement that (unfortunately) holds for extremism and terrorism research. Computational methods now routinely allow researchers to provide extensive network maps of extremist ecosystems,[8] evaluate users' behaviours and influence,[9] and analyse very large quantities of texts found on online spaces to identify their main themes or track ideological evolution across time.[10] Among these tools, machine learning techniques are increasingly described as constituting a particularly useful toolkit for the detection and analysis of vast amounts of online extremist data.[11]

However, what is arguably the prime component of communication in today's extremist ecosystems – visual imagery – has remained largely untouched by researchers using computational methods. This is not surprising: the visual dimension of extremist online spaces and their ecosystems has only recently attracted sustained academic consideration, and has thus received scant attention in methodological reviews and reflexions. Schuurman's 2020 review of methods in terrorism research revealed, among others, that "online content" (including non-visual material) and "media (film)" only constitute about six percent of published scholarship; the words "images" and "visual" don't even feature in the review. A recent special issue of *Studies in Conflict & Terrorism* dedicated to methods in terrorism studies did not include a contribution specifically dedicated to the study of imagery. Visual methods are similarly absent in terrorism research methods manuals,[12] and rarely feature in general political science methodology textbooks.[13]

Yet visual analyses of terrorism and extremism do exist and are gaining in popularity, already yielding important insights mostly through qualitative or "quasi-quantitative"[14] methods investigating small samples. While this is a welcome development, we argue here that, given the large empirical universe warranting analysis, much is to be gained by complementing these traditional approaches with computational analysis, doing for images what has already been done for text. ISIS, for instance, published almost 15,000 photographs and more than 1,700 photo reports between October 2014 and October 2015,[15] and this already large quantity only equates to the volume of images shared daily on certain far-right sites, forums, and social media accounts. The situation is now exacerbated by the multiplication of digital bots and AI-generated imagery.[16] The argument we make, therefore, closely parallels the one made by Grimmer and Stewart ten years ago in their seminal *Text as Data* article,[17] and extends Joo and Steinert-Threlkeld's recent *Image as Data* contribution, which transposed the former's logic to the computational study of images in political science broadly speaking.[18] As Joo and Steinert-Threlkeld argued, "images are key drivers of political phenomena, and we would do well to take advantage of new techniques to analyse them in large quantities in research".[19] In this paper, we follow and deepen this line of thought to tailor it to the field of security, terrorism and extremism studies, examining how it adapts to the specificities of extremist/violent political actors' communications. Specifically, we clarify how unsupervised and supervised visual computational methods work, explain how recent advances in some of these methods have drastically reduced the resources required for their implementation,[20] highlight the advantages and limitations of these methods when it comes to investigating large-scale visual extremist corpora, and specify the role of these tools to complement existing qualitative approaches within mixed-methods research designs.

To do so, we proceed in three main steps. First, we situate our endeavour within the relatively recent effort to study the visual component of extremist online spaces, tracing it back to the "visual turn" in International Relations, security studies, and terrorism research. Recognising the merits and strengths of this endeavour, we also reassert its shortcomings in a context marked by the hundreds of millions of images populating increasingly vast extremist ecosystems. Second, we succinctly explain in lay terms what computer vision is, distinguish between two main variants (unsupervised vs. supervised), and deploy one method from each of these approaches (unsupervised clustering vs. supervised object detection) on an original extremist visual corpus – more than 30,000 images collected from the incelosphere – in order to illustrate their logics and performance. Finally, we reflect on these empirical findings to reflect on the strengths and limitations of computational visual methods for the study of online extremism and terrorism, situating these tools within a coherent research workflow alongside non-computational approaches.

## Strengths and Limitations of the "Visual Turn" in Extremism and Terrorism Studies

Extremism and terrorism scholars' recent awakening to the importance of visual imagery is inspired by a longstanding line of research in visual anthropology and sociology, and reflects similar undertakings in neighbouring fields, such as political communication[21] and IR and security studies,[22] where "the explicit study of visual politics has only recently begun to coalesce into a recognized area"[23] and ambitious research agendas are now set up to unpack the multiple implications of the "visual age". Following suit, extremism and terrorism studies are now starting to correct their biased "emphasis on understanding the words contained in the groups' messages rather than images"[24] and tendency to "focus on textual aspects and overlook the visual".[25] Taking stock of pioneering interventions, such as Bolt's *Violent Image* book,[26] Doerr's framework for studying visual mobilisation in conflict,[27] or Dauber and Winkler's edited volume exploring *Visual Propaganda and Extremism in the Online Environment*,[28] a much-needed "visual turn" implementing a clear research agenda was called for by Maura Conway in an influential 2019 blog contribution.[29] As she aptly summarised, "the heavily visual nature of today's violent extremist online spaces makes this a real problem for us going forward however: we must do better."

The problem is, indeed, a thorny one: analysing extremist and terrorist imagery presents a range of difficulties that explain why scholarship has not taken off earlier or been more extensive. Storing (let alone sharing) images from terrorist organisations is prohibited or severely constrained in most research-intensive countries, pictures are often gruesome or shocking, the proximity of several extremist ecosystems (e.g. incel, far-right) with other fringe digital milieux (such as pornography or child abuse) means that visual datasets are often "contaminated" by problematic, unwanted, and, at times, illegal images, and, as highlighted earlier, strong visual methods are not a well-established part of the standard toolkit. Additionally, today's highly dynamic digital environments mean that images, such as memes, are not static singifiers and constantly evolve as they spread,[30] often resulting in shifting meanings or situations where the image itself being adapted in multiple ways (the prime example of this in extremism research is the "Pepe the Frog" meme, discussed below). Computational techniques have additional issues, well presented in Scrivens and colleagues' recent exposé on the challenges of online data collection in terrorism and extremism research: they involve technical skills, face opaque and ever-moving access points to platforms APIs, necessitate large storage spaces, and sometimes expensive hardware (such as servers or GPUs) and suffer from off-the-shelf commercial crawlers' inability to harvest pictures.[31]

Despite these difficulties, studies of the visual dimension of extremism and terrorism have emerged and typically belong to one of two types of what we could call *human* methods, in contrast to the *computational* methods presented below. In the first type, one or several visual tropes are hand-coded in all or (more likely) a sample of images constituting a visual corpus. This approach allows for measuring how frequently this/these tropes occur within, typically, a few hundred images (rarely beyond the thousand). In the second type, an in-depth interpretive analysis of one or a handful of particularly important, iconic image(s) is conducted to explain their symbolism, communicative function, embedded narrative, or/and emotional appeal. The first approach is more suited for studying the manifest meaning of images (e.g. the image contains a particular object or symbol), while the second is more apt at uncovering latent meaning (that is, meaning not immediately apparent but produced through the interplay of the image content and its cultural and ideological contexts and subtexts). Both types of analysis are usually deductive, in the sense that they rely on theoretical frameworks (be it from sociology, philosophy, media studies, etc.) to infer which visual tropes are *a priori* important, and subsequently look for them. However, a dose of induction is almost always present as experts make educated guesses based on previous encounters with similar datasets as to what types of images could be critical or frequently occur, sometimes at odds with theoretical expectations.

These two human methods have delivered important empirical insights when it comes to extremist and terrorist imagery. Among them, five stand out. First, each terrorist or extremist group has a specific visual style, understood as its "basic choice of the content and type of narrow visual landscape it tends to favor", and this style is sensitive to external (e.g. material constraints, political environment) and internal (e.g. leadership change, ideological evolution) shifts.[32] Baele, Boyd, and Coan's study of ISIS's visual style, for example, examined the chronological variation of four visual tropes in the organisation's imagery,[33] which has since been examined with much greater depth by Winter in a decisive volume dedicated to terrorist imagery.[34] Second, recurring images – such as those of "good Muslims" in ISIS magazines,[35] ideal citizens facing a threatening "other" in the Danish People's Party's internet,[36] or "strong virile white farmers, traditional earthy homesteading moms" in neo-Nazi Instagram accounts–[37] play a key role in the construction of ingroup and outgroup stereotypes and "socially typified personae",[38] creating "a divide between the in-group and purported out-groups",[39] and constructing an underlying "moral order".[40] Third and more broadly, the array of visual tropes being used by extremists and terrorists is not vast; a limited number of image types is present across ideologies, each serving a particular function in outreach and subsequent radicalisation. Besides stereotypical images of ingroup and outgroup members, both symbols and gruesome/grotesque imagery –[41] including the "about to die" image[42] and more generally the "death" representation –[43] feature regularly.[44] Fourth, visual icons travel across national contexts, with processes of "translation" undertaken to make them resonate with local audiences and stakes. For instance, Doerr traced the itinerary of the "black sheep" poster from its initial Swiss context to its subsequent variations in Italy and Germany,[45] and more recently studied the recycling of US Capitol uprising images by German far-right movements.[46] This dissemination/translation process can even occur across ideological boundaries; for example, Miotto showed the similarities between jihadist and far-right visual representations of martyrdom.[47] Finally, sharing and consuming extremist imagery is, from a perspective inspired by Bourdieu and other sociologists, a social practice that participates in processes of group affiliation, self-identification, positioning, and emotional bonding, and thereby radicalisation. DeCook has, for example, shown how the display and dissemination of memes and other forms of images constitute key socialisation practices among the Proud Boys.[48]

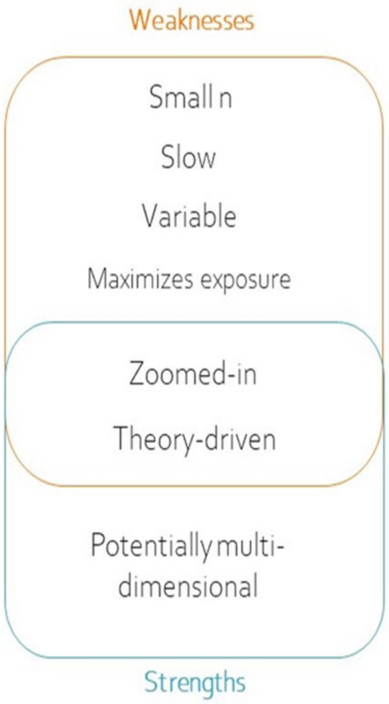
Three key strengths of human approaches have unlocked these insights. First, as mentioned, they are usually theory-driven. This means that they are geared to producing immediately relevant findings determined by the expert's conceptual understanding and research prioritisation. Second, they are excellent at offering careful characterisations and in-depth interpretations of the specific, delineated visual landscape on which the expert zooms in. Third, they allow for multi-dimensional evaluations and interpretation of latent meaning, both in the sense of attuning to images that combine several visual tropes in sometimes subtle or even cryptic ways, and in the sense of permitting the simultaneous investigation of several visual tropes. Miotto's or Doerr's abovementioned studies provide good examples of the kind of granular, interpretive scrutiny of extremist images and visual landscapes that human approaches can offer.

Yet, as Conway suggested, we can do better. These standard human methods indeed have four important limitations. First, they are not adapted to the contemporary extremist visual environment characterised by millions of images of many sorts (pictures, memes, caricatures, image-text collages, etc.). While hand-coding can be done on small coherent samples or even full corpora (e.g. all images contained in ISIS magazines or on a given far-right blog), small-n human methods are simply incapable of scaling up and gaining a panoramic view of the visual landscape. As Bleiker puts it, "methodological issues get exponentially more difficult" in a situation characterized by "a limitless number of images".[49] Engstrom's study of images from the British National Party is a case in point:[50] having gathered over 10,000 "visual elements" from its website, he had to restrict his analytical lens to only 600 images of a certain type, thus leaving aside 9,400. Second, human methods are slow, making them inadequate for a digital context characterised by a fast turnover of images (new ones constantly appearing, established ones regularly morphing, etc.). Commercial services specialised in coding images do exist and work relatively fast (some even have in-house coders familiar with extremist environments), but relying on them for monitoring projects can become onerous and expensive, and they will always be slower than a machine. Third, while human methods have the advantage of relying on human intelligence, they also incur variability. While inter-coder reliability is usually high for unambiguous, easily identifiable items (such as the presence/absence of weapons or a particular symbol in an image), scores inevitably drop as soon as a degree of interpretation is needed. For example, reliability scores in Baele, Boyd and Coan's abovementioned paper were almost perfect when it came to identifying pictures with symbols or gruesome elements, but much lower when it came to selecting the narratives conveyed by the pictures. As a result, some scholars only look at unambiguous tropes, avoiding potentially more insightful aspects,[51] or provide results that are hard to replicate. As Joo and Steinert-Threlkeld explain, these last two weaknesses alone explain why visual studies have traditionally been highly qualitative, focusing mostly on a few iconic images.[52] Finally, sustained close examination of extremist corpora maximises researchers' exposure to potentially harmful content (gruesome imagery, graphic violent porn, etc.). This is a major issue in our field, where researcher's wellbeing has long been ignored and exposure to this extreme content has become increasingly frequent.[53]

Additionally, we argue that some of the strengths of the human methods can also be limitations. On the one hand, the usually deductive character of these approaches means that scholars may miss crucial yet theoretically unexpected dimensions. Dominant theories or the community doxa inevitably drive our empirical attention towards particular types of images, yet in a fast-moving visual landscape, other pictorial genres might have gained prominence regardless of our pre-existing concepts. On the other hand, while zoomed-in investigations of specific visual styles and landscapes allow for granular, in-depth understandings of particular visual landscapes, they are, by design, blind to the (very) big picture. Discussing interpretive versus automated text analysis, Hart usefully compared the former with sightseeing a city on foot and the latter with viewing this city from a helicopter, both approaches are needed to gain a full understanding of the place.[54]

In sum, the strengths and weaknesses of human methods for visual analysis in extremism and terrorism studies can be represented as in Figure 1 below.

*Figure 1. Strengths and weaknesses of human visual analysis methods.*



# Deploying Computational Visual Analysis in Extremism and Terrorism Research

For about two decades now, the shortcomings of human methods for the analysis of *textual* extremist corpora have been addressed by supplementing them with computational tools, and we suggest that recent developments in computational methods mean that the same logic should now be applied to *visual* ones. Indeed, the fast developments of machine learning methods in recent years have made computer vision faster, more accurate, and more sophisticated than ever before. In the following paragraph, we briefly define computer vision and identify its two most pertinent applications when it comes to extremism and terrorism studies (object detection and clustering), which we operationalise using original visual data from incel online spaces. We then build on this exploration to summarise, in the same way we did for human methods, its strengths and limitations when applied to extremist and terrorist content.

## *Computer vision*

Computer vision can be defined as the "subfield of AI that enables computers and systems to process visual data, such as images and videos, and generate patterns for detecting, tracking, and classifying objects".[55] In other words, the primary goal of computer vision is to "replicate human visual abilities with computational models".[56] Pushed forward by major breakthroughs, such as Krizhevsky, Sutskever, and Hinton's "ImageNet",[57] the technology of automatically recognising patterns in visual environments has by now taken an important place in everyday life: applications include running autonomous cars' navigation systems, allowing crop monitoring by drones in large farming estates, recognising faces in surveillance systems, and detecting patterns that diagnostic specialists don't see in medical imaging. Computer vision models can be either *supervised* (presented with a training dataset wherein the programmer has labelled visuals deemed important) or *unsupervised* (in this case, the model is set up to detect patterns without guidance).

Computer vision is slowly making its way into political science and media studies, paving the way for applications in our field. For example, large corpora have been automatically mined to better understand how politicians present themselves on social media (and how these self-constructions correlate with ideological positioning[58] or convey particular emotions),[59] or how political memes circulate across social media.[60] Similar tools have very recently started to be used in extremism and terrorism research, yielding important findings. In a noteworthy contribution, Zannettou and colleagues designed a "processing pipeline" aimed at identifying and tracking the online dissemination of far-right memes, combining computer vision techniques such as clustering with other computational tools; deploying this pipeline to 160 million images from sub-Reddits, Chan boards, and Gab channels demonstrated not only the performance of the method but also the novelty of the perspectives gained through computer vision. Finkelstein and colleagues subsequently applied the same process to evaluate the frequency of the "happy merchant" meme (detected automatically in over 7 million images from a range of far-/alt-right online spaces), used as a proxy for antisemitism, and measured how this meme has gradually "infected" other visuals in memetic combinations (appearing together with the likes of Pepe the frog or Wojak in single images).[61] Using a different approach, Crawford, Keen, and Suarez-Tanguil categorised more than 135,000 images from various Chan racist boards into several types to help define their "visual cultures",[62] while O'Halloran and colleagues used qualitative multi-modal annotation to direct large-scale AI detection of ISIS-related images and text.[63] Despite their merits, these breakthrough studies remain rare and scattered, are usually published in computer science outlets, and their exact role or contribution within the field is rarely unpacked. For this reason, we try to expose as clearly as possible for the non-expert audience the strengths and weaknesses of the two types of computer vision models holding, we argue, the most promise for extremism and terrorism studies, and on that basis we nail down their role in the field.

## Data

To illustrate these methods and ground the discussion in the empirical reality, we use a corpus of more than 32,000 images featuring in posts extracted from nine different online spaces (spread across three platform types) pertaining to the so-called "incelosphere" (see Table 1 below).[64] The images were collected using a series of custom-built web-scrapers developed in the Python programming language, utilising common packages, such as *ScraPy* (https://scrapy.org/) and *Requests* (https://pypi.org/project/requests/). Depending on the platform, various APIs were used to aid data extraction where appropriate (i.e. the Telegram scraper utilised the Telethon API; see https://docs.telethon.dev/en/stable/). While definitely at the lower end of the size scale that computational methods are called to handle, this corpus possesses two advantages for the purpose of this article: firstly, the visual landscape of the incelosphere has not yet been thoroughly studied, meaning that we demonstrate our conceptual points on a novel case, and secondly, this is a hard case against which to test the computers, meaning that the corpus images appear highly diverse, cryptic, and regularly shocking.

*Table 1. Corpus statistics: Number of images extracted from each incel online space.*

| **Source of images (Online space)** | **Platform type** | **Number of images extracted** |
|---|---|---|
| 4chan/R9k | Chan board | 25,747 |
| 9chan/Leftcel | Chan board | 1,744 |
| BlackPillsBasedGlobal | Telegram | 1549 |
| Blackpilled | Telegram | 376 |
| Incel | Telegram | 877 |
| IncelsCo | Telegram | 624 |
| _incels_ | Instagram | 18 |
| B_l_a_c_k_p_i_l_l_e_d | Instagram | 49 |
| Blackpillmemez | Instagram | 525 |
| Involuntarycelibacy | Instagram | 212 |
| #Blackpill | Instagram | 866 |

## Image clustering

A first type of computer vision model perform *clustering*, which consists of "grouping together similar items into distinct clusters, so items within a single cluster are similar to each other and different from items outside the cluster."[65] In other words, clustering seeks to "partition observations into mutually exclusive categories, or clusters, using principles of unsupervised dimension reduction."[66] As such, this visual analysis technique is akin to unsupervised topic modelling in text analysis: it inductively "reveals" the major dimensions and tropes of a large corpus, allowing the researcher to "let the data speak". Four more specific similarities between text topic modelling and visual clustering illustrate the nature and relevance of the tool. First, like topic models, a range of algorithms are available when it comes to visual clustering (e.g. Affinity Propagation, Agglomerative Clustering, K-Means clustering), each implementing a different strategy for calculating visual distance/closeness and the subsequent grouping of images. Each comes with its strengths and limitations and higher/lower pertinence for particular corpora and research objectives. Second, just like the number of topics can be suggested by the researcher conducting a text analysis, some visual clustering models require users to pre-define a given number of clusters, for the computer to subsequently calculate the optimal categorisation of images within them. Third, by assigning each image a class/category, visual clustering algorithms offer a quantification of which ones of these categories are particularly prominent in a corpus; the researcher is thus able to quickly see which types of images are (not) frequent. Fourth, although visual clustering models are unsupervised, their application to specific types of imagery can be preceded by training with a narrower visual dataset similar to the one to be examined, which increases their robustness.[67]

For these reasons, this tool is particularly useful in two strategies. First, it can help researchers gain a general overview of the visual landscape under investigation, with the main types of images appearing together in groups with measures of their respective importance. Just like a text topic model provides a quick understanding of the major themes of a corpus, a visual clustering model offers a rapid panorama of its visual landscape. This strategy is particularly useful for new and very big corpora for which little is known, i.e. where no "natural" categories are yet known. As Grimmer and Stewart explain in their work on unsupervised text topic modelling, while supervised methods assume a well-defined set of categories (inferred from existing scholarship or theoretical hypotheses), in some cases that set of categories is hard to derive beforehand.[68] Second, it could be used as a way to gain new, original knowledge of a big corpus which tends to be repeatedly appraised through the same lenses. Dominant theories (or doxa) that consistently direct empirical studies towards a limited number of visual tropes are at risk of being blind to important but unaccounted aspects, and biased in favour of particular features that may actually be found only in a minority of images. To use Grimmer and Stewart's work on unsupervised text analysis again, these "methods are valuable because they can identify organizations of text that are [...] understudied or previously unknown".[69] This second strategy is, therefore, most useful when dealing with large corpora that have already been investigated by researchers using similar theoretical frameworks and associated methods, as a way to avoid bias and unlock new knowledge.

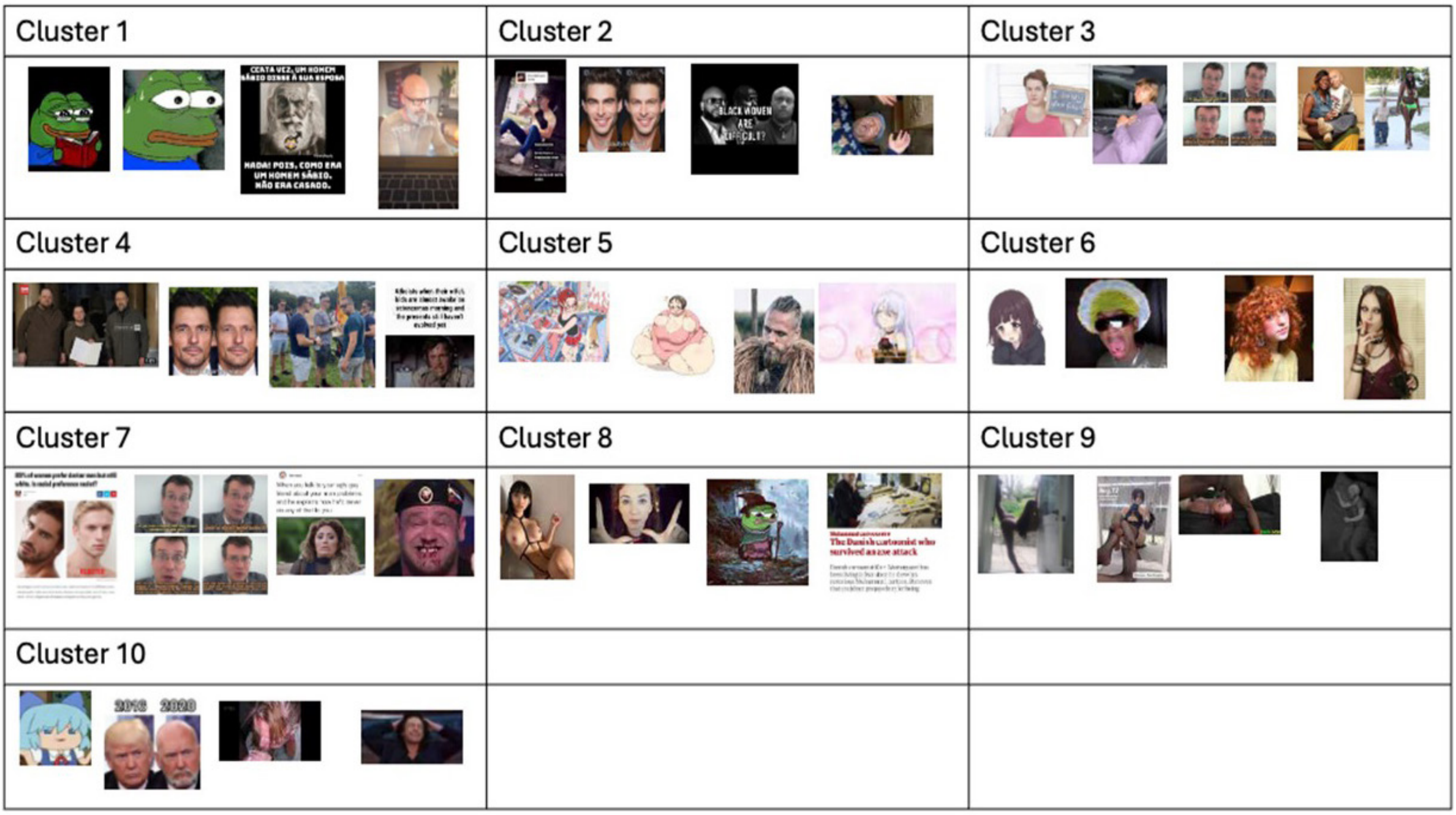
Following the successful application of this method to large visual political corpora (including Joshi and Buntain's clustering of 15,000 images posted on social media by over US politicians, which demonstrated that the types of images shared by these politicians were a "strong indicator" of their ideological position),[70] we ran a deep image clustering algorithm on our visual corpus. We used the Unsupervised Deep Embedding for Clustering (DEC) model, as originally proposed by Xie and colleagues.[71] In recent years, DEC models have proven themselves effective at clustering images into groups within large datasets. However, it has also been shown that the relationship between the models' convergence and their hyperparameters is tricky, and therefore requires multiple runs with different hyperparameter settings to achieve the optimal grouping. Crucially, there are no rules for finding the "best hyperparameter values". Instead, the researcher must ascertain this themselves through experimentation (and substantive expertise) with the number of *epochs* and *batch size* (the former refers to the number of passes made over the whole dataset, and the latter refers to the number of individual images the model sees before being updated).

It is therefore recommended that a test set is ready to evaluate the model's output after training., as although increasing the number of epochs will tend to increase accuracy, this might be the result of overfitting (i.e. the model is fitted too closely to its training data and therefore unable to make predictions when presented with new data). Having a test set of data that the model has never seen before allows to validate the model's outputs. To demonstrate the importance of this, we trained the DEC model on the 32,587 images of our corpus for a number of different epochs and batch sizes. Two observations can be made from Table 2 below. First, the highest amount of accuracy in predictions on the test dataset that this model is able to achieve is 31 percent. Second, this is achieved using a batch size of 32 (the default batch size for most open-source model implementations), and increasing the number of epochs does not improve this. Indeed, the model only achieves 21 percent accuracy with 50 epochs at 32 batch size, but hits its highest accuracy with 100 epochs, and does not improve beyond that. We can, therefore, see that our model follows the traditional wisdom of the machine learning community, in that having more epochs does not necessarily equate to a more accurate model.[72] We can thereafter conduct a visual inspection of these results by extracting a sample of images from each cluster. Looking at Figure 2 below, we see that a model trained for 20,000 epochs with a batch size of 32 has started to create some coherence, with Pepe memes appearing a lot in cluster 1, and clusters 2 and 5 containing mostly pictures of men and anime girls, respectively.

*Table 2. Comparison in accuracy at predicting data test dataset (from our incel visual corpus) for various epoch and batch size values.*

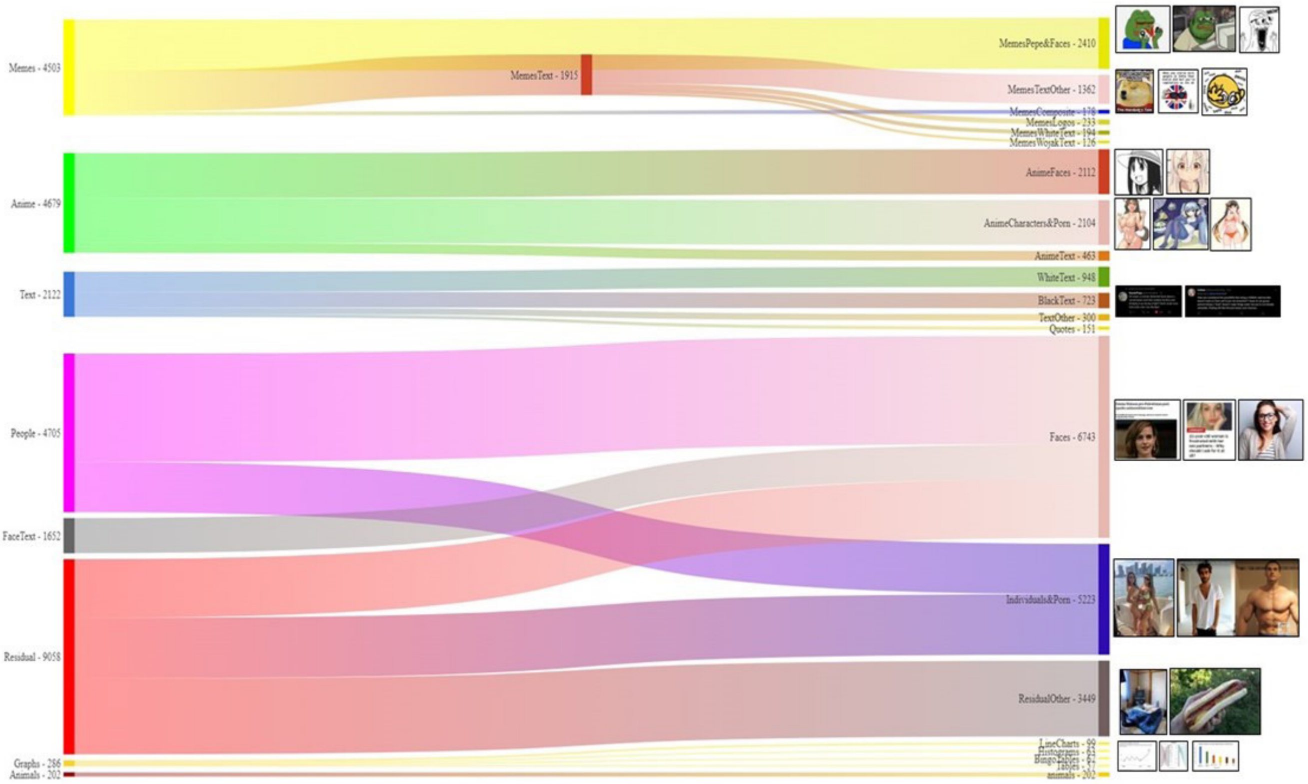
| Number of epochs | Batch size | Accuracy |
|---|---|---|
| 50 | 32 | 0.21 |
| | 100 | 0.05 |
| 100 | 32 | 0.31 |
| | 100 | 0.18 |
| 500 | 32 | 0.31 |
| | 100 | 0.08 |
| 2,000 | 32 | 0.31 |
| | 100 | 0.04 |
| 20,000 | 32 | 0.31 |
| | 100 | 0.03 |

*Figure 2. Test clustering with ten clusters of incel images.*



Clustering, therefore, rests on a series of trial-and-error, back-and-forth steps seeking to increase coherence, estimated not only mathematically but also through the lens of the researcher's substantive expertise. Importantly, clustering can also be re-run within clusters – for example, one could run a model within a hypothetical "vehicles" cluster to see whether the machine identifies and separates cars, planes, etc. We adopted this strategy with our whole corpus to increase coherence, and the results are presented in Figure 3 below. This is a graph inspired by Rogers' suggestion to create "metapictures", that is, ordered displays of collections of images scraped from social media in arrangements such as "tree maps" or "cluster maps" that allow for rapid scanning and critical reflection (this approach "nestles itself between qualitative visual analysis and interpretation […] and quantitative knowledge visualization").[73] We can see that this strategy improved coherence, with the computer for instance grouping all meme characters together, as well as anime faces, anime porn characters, or graphs/ figures. Appendix 1 offers another example using a different corpus, to provide an extra illustration beyond the specific case at hand here.

*Figure 3. Clustering diagram of images from the incel online ecosystem.*



Four observations can be made on the basis of our application of visual clustering to the images contained in our corpus. First, the tool's ability to quickly gain a zoomed-out overview of a large visual landscape is confirmed. With no existing scholarship on incel visual imagery, our incel cluster map reveals three major types of images populating the incelosophere: people's faces (mostly women's), anime (mostly girlish characters, regularly in sexualised or pornographic), and individuals (incels, "chads" and "stacies").[74] These proportions reveal the community's valued pictorial practices (e.g. sharing erotic/pornographic and anime images, or photos of particularly attractive/repulsive individuals) and offer an indication of its major themes and ideological tenets (e.g. "lookism").

Second, the clustering tool is, as anticipated, useful for disclosing new patterns not foreseen by theory or the literature. As noted above, the scholarship on extremist visual imagery tends to concentrate on the role of symbols and in-/out-groups depictions and, more recently, memes (which, in a sense, merge symbolism with group identification). Even though the importance of group portrayal is confirmed in our data, the cluster map also shows that cartoonish memes are not (quantitatively) a crucial visual genre, and reveals pictorial types so far ignored by the literature yet obviously empirically and theoretically relevant (e.g. “scientific” graphs, figures, and infographics).

Third, the tool’s fully inductive logic inevitably produced residual clusters that are frustratingly irrelevant, theoretically speaking, with the “image-text” genre derailing parts of the process in the far-right case provided in Appendix (note that some AI models are geared at isolating images from their added texts). While theory blindness does bring about novel, unforeseen insights and observations, it comes at a cost when complex visual corpora such as the incel one are involved, which contain composite imagery for which other computational tools are required.

Fourth, the output clearly calls for additional, fine-grained research in the form of human methods (small-n hand-coding, very small-n interpretive analysis). The incel cluster map, for instance, groups together visibly different images of women serving distinct functions for the incel community and worldview that ought to be investigated.[75] As we discuss below, this method is, therefore, best used as a tool for preliminary data exploration.

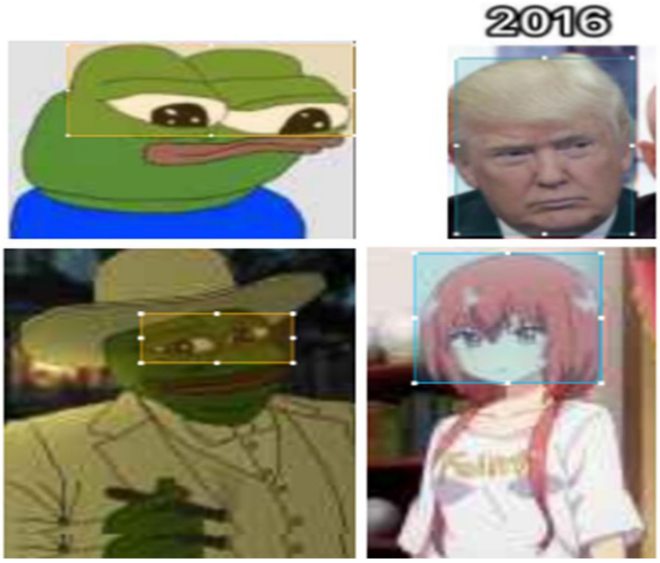
## *Object detection*

The second type of computer vision model we highlight here performs *object detection*, that is, the “task that deals with detecting instances of visual objects of a certain class (such as humans, animals, or cars) in digital images”,[76] or, put differently, the “task of predicting the class and the location of different objects contained within an image.”[77] The past decade has witnessed “a rapid technological evolution of object detection and its profound impact on the entire computer vision field”,[78] mostly due to the application of sophisticated deep learning techniques that led to a leap forward in models’ accuracy and speed,[79] including when detecting objects on moving images (videos, real-time footage). There are two types of deep-learning object detectors, which reflect developers’ preferences on either end of the accuracy/speed trade-off: “two-shot” models privilege accuracy by first finding potential objects in an image and then classifying each one of them (e.g. “car”, “person”), while “one-shot” models privilege speed by merging the two tasks.

Object detection is useful in two different research strategies. First, it can be used to offer a broad-brush understanding of the relative importance of a large range of standard objects in a large corpus: does this dataset contain, for example, lots of images of infrastructure/buildings or vehicles? In extremism and terrorism studies, models can quickly detect specific types of theoretically relevant images in a large visual corpus, automating (that is, speeding-up and scaling-up) what would have otherwise been a tedious hand-coding process. For example, pre-trained models automatically detect firearms in images, and models further trained on weapons are able not only to detect them but also to distinguish, in real-time video recordings, between different types of guns, rifles, knives, etc.[80] Second, models can be custom-trained to detect, and measure the prevalence of a limited number of highly specific and relevant categories of objects; i.e. Nazi symbols, ISIS magazine covers, pictures of known terrorists, particular versions of a well-known meme like Pepe the frog wearing an SS uniform, etc. Such custom-trained object detection models, which require researchers to manually code classes and their locations within images with a bounding box, are better suited to detecting specific imagery compared to unsupervised approaches, such as clustering. They are a useful tool for a range of different study designs; for example, they can ground an evaluation of the ideological character of an online platform or serve as a measure of the ideological evolution of a given online platform or ecosystem over time (e.g. does it contain an increasing/decreasing quantity of Nazi symbols?).

To demonstrate how useful object detection models can be in studying extremist online communities, we utilised a one-shot model known as YOLO (acronym for "You Only Look Once"). Originally developed by Redmon and colleagues,[81] YOLO models depart from other object detection models that repurposed classifiers for the task of object detection, and instead treat the task as a regression problem between bounding boxes and class probabilities. This is achieved by using a single convolutional neural network (CNN) to predict both boxes by looking at the full image in one go, meaning that predictions are based on the global context of the image. YOLO is one of the most popular object detection models, due to its high level of accuracy and speed – two qualities that have made it particularly suitable for real-time applications. Given that this is a supervised learning approach, meaning that the model is presented with both training images and their associated labels as to what classes (i.e. "man", "woman", "pepe") are contained within the image and their location, the first step in developing a custom-trained object detection model is to build the training dataset. The final training dataset will consist of the images you wish to train the model on, whereby for each image there is a text file in which each line details a class and the location of the box that contains the class instance. Creating this training dataset involves manually assessing each image and creating a corresponding bounding box for any of the classes that the researcher wishes their model to detect, with these bounding boxes being where the class appears in the image.[82] Figure 4 below provides an example of what this process looks like for four different images. This time-intensive process of labelling classes in training images means that, despite the significant impact supervised object detection models could have for extremism researchers, there are some aspects that researchers with limited resources might struggle with.[83] However, new models still get increasingly powerful, continuously reducing the time and expertise needed for training them. In our case, YOLO proved powerful enough to learn specific theory-relevant objects on a relatively small training dataset.

*Figure 4. An example of manually created bounding boxes for three different classes in four images.*



Specifically, we followed a two-step training process using 11,700 images randomly selected from the whole corpus, in order to ascertain what our classes of interest would be. First, 4,000 images from the random sample of 11,700 were (again randomly) selected and evaluated for potential classes of analytical interest (i.e. classes that appeared regularly enough and/or contained some known specific meaning within the incelosphere), which was done in order to control for the fact that many of the incel images were random in nature and did not have any real significant meaning or content to them. The results of this step were then evaluated, with the frequency of each class being assessed and removed if it was below ten;[84] this resulted in twelve classes. In a second step, we took these twelve classes and labelled any instances of them that appeared in the 11,700 sample by creating a bounding box as detailed above. This resulted in a total of 3,620 labels across 2,808 images (detailed in Table 3 below); 8,892 images contained miscellaneous content that did not fit into any of the twelve classes of analytical interest. Once complete, the labelled images were divided into 2,307 training and 501 test images.

*Table 3. Frequency of instances per class in the incel training dataset.*

| Image category label | Number of ground truth boxes |
|---|---|
| Man | 1066 |
| Anime girl | 783 |
| Woman | 656 |
| Social media post | 324 |
| Pepe | 270 |
| Nude woman | 146 |
| Wojak | 115 |
| Porn | 111 |
| Military | 61 |
| Chad | 60 |
| Trad girl | 15 |
| Swastika | 13 |

An instance of Ultralytics' YOLOv8[85] was then implemented and trained on the sample for 500 epochs, yielding impressive results given the small dataset it was trained on (see Appendix 2 for additional information on validation metrics). Figure 5 below shows a precision-recall curve graph, which plots the precision and recall in our model for each of the classes for all possible user-defined thresholds between 0-1. Ideally, precision and recall would be high (in other words, the model detects all instances of a category, and what it detects is correct). However, in reality, there is a trade-off between precision and recall since a lower threshold decreases the chances of ground truth boxes being missed since this would increase the number of detections made by the model, but at the same time, a higher threshold would mean that the model is more confident in what it predicts. Thus, a precision-recall curve is useful in ascertaining what the user-defined threshold should be, depending on the desired application of the model. In Figure 5, we show the conditional probability that the bounding box belongs to the specific class it is next to. For the purposes of this paper, we will also use a probability of 0.5 to signify a hypothetical baseline model; in other words, like logistic regression, if an instance is believed to belong to a specific class with a probability of >0.5, it is tagged as positive. This baseline model is represented by the grey dashed lines. Figure 6 below additionally supports what we see in Figure 5. Figures 7 a, b, and c below, which are collages of predictions our trained model made on the 501 test images (i.e. images that the model did not see during training), also allow for manual inspection of the model's accuracy.[86]

*Figure 5. Precision-recall curve for the custom-trained YOLOv8 model trained on the incel dataset.*

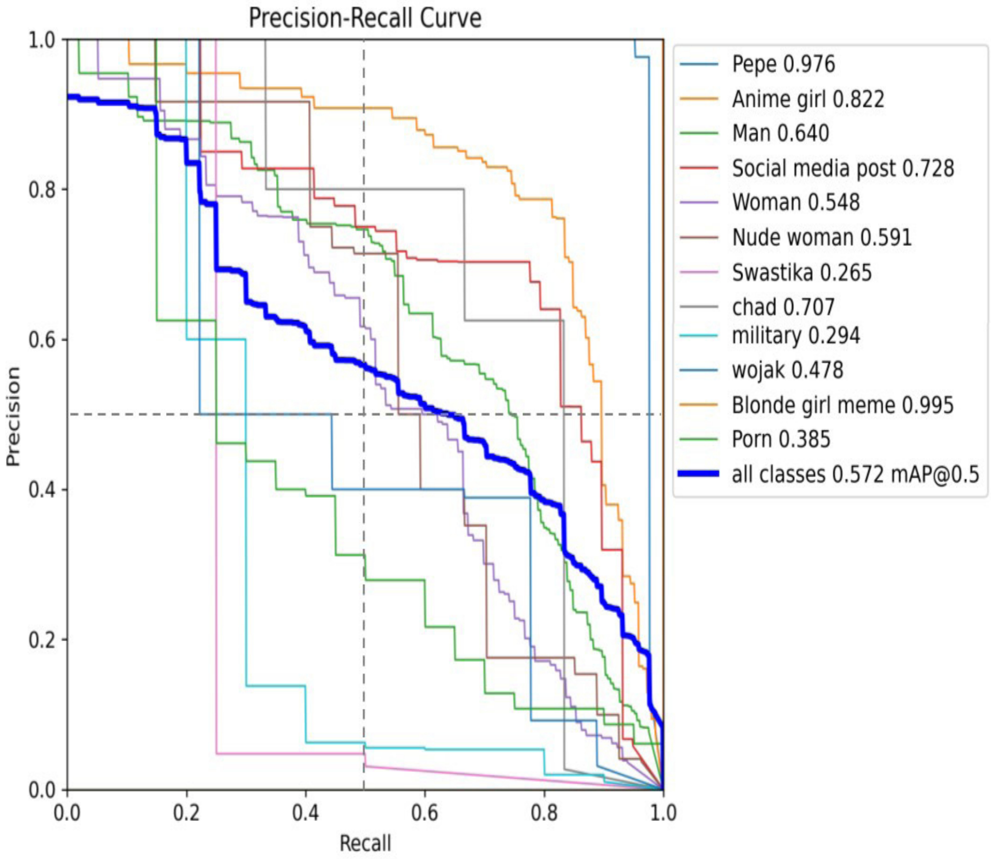
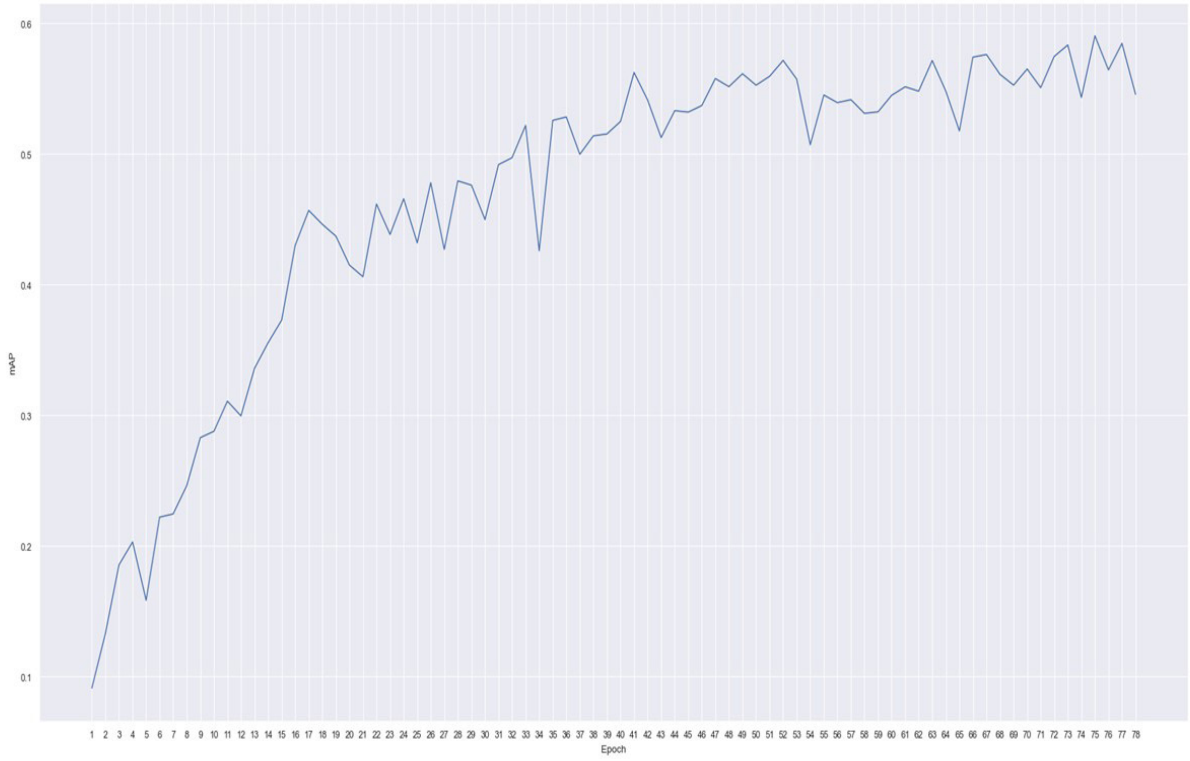


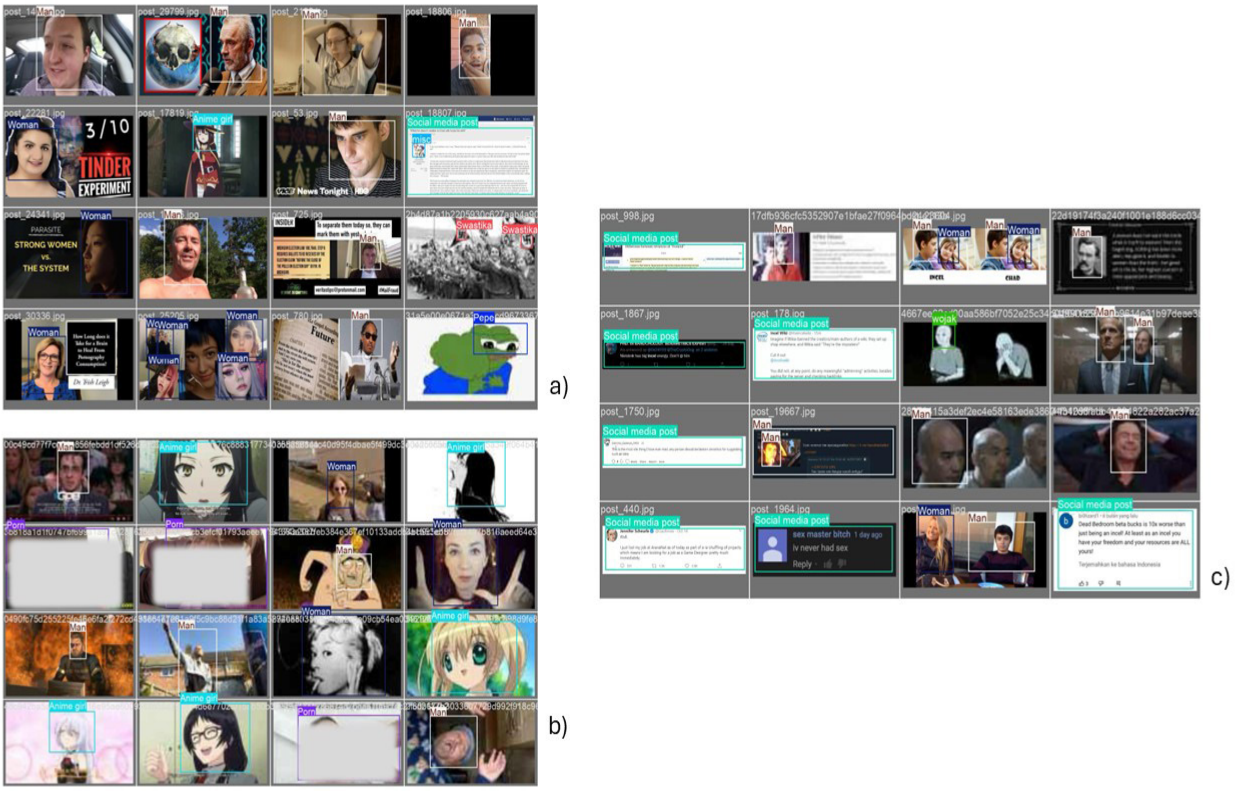
*Figure 6. mAP score for the custom-trained YOLOv8 model across epochs (1-75).*



Looking at Figure 5, we can see that the model has developed near-perfect precision recall for both the "Pepe" (0.976) and "Trad girl" (0.995) memes (their respective lines almost follow the exact shape of the top right-hand corner of the graph box). The high confidence value for these two memes shows the importance of thinking about bounding boxes when undertaking an object detection project looking at memes. Namely, as stated above, within the incel (and many other) online subcultures, the same memes often appear in different forms. This is particularly true with the Pepe meme, which is not only shared in its "base form" but is also wearing hats, having facial hair, sometimes having a whole body, and many other forms. This can make it difficult for this image to be detected by computer vision algorithms. However, due to the use of bounding boxes in object detection, we were able to specify that the model should look for a specific part of a meme to detect it — in this case, the bounding boxes were set to the Pepe character's eyes as these were, in a sense, the smaller common denominator in the vast majority of Pepe meme iterations (cf. Figure 4 above). As can be seen in Figure 7 a below, this enabled the model to accurately detect this meme, despite its numerous forms and only 270 coded instances of it in the training dataset. Impressively, the model's success in finding Trad Girl memes rested on only 15 coded instances in the training dataset; here the model's power was aided by the fact that this meme has unique visual features and appears with little variation in the dataset.

The model also proved to be quite effective at detecting other classes. With 783 instances in the training dataset, the model developed a 0.822 confidence score for the "anime girl" class, likely due to the highly stylised nature of these images (i.e. large eyes and pointy hair). With a confidence score of 0.728 based on 324 training instances, the model detected social media posts well; it also proved relatively successful at detecting headshots of both men (0.640 confidence with 1066 training instances) and women (0.548 with 656 training instances). As can be seen in Figures 7 a, b, and c, unlike the three classes above, these classes are characterised by high variability (ethnicity, facial hair, head hair, glasses, etc) without any stylised and uniform characteristics, and would, therefore, require more training instances in order to improve the confidence score. Further, the model was able to achieve 0.591 confidence with the nude woman class based on a very small set of 146 training images, a testament to the YOLO approach given the large amount of variation between different training instances in terms of poses, etc. Likewise, a confidence level of 0.707 with only 60 training instances for the "Chad" meme is impressive. The rest of the classes fall below the 0.5 confidence of our hypothetical baseline model, but Figures 7 a, b, and c nonetheless show that some predictions are accurate. In these cases, more training instances are required to allow the model to handle variations within a single object deemed relevant.

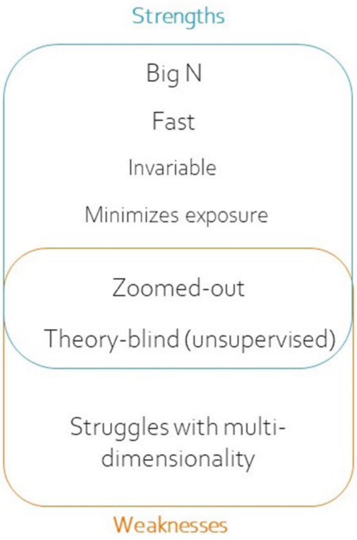
*Figures 7 a, b, c. Collages of validation images showing some of the predictions made by the custom YOLOv8 model.*



## Capitalising on Strengths, Acknowledging Weaknesses: Towards a Research Workflow Integrating Computer Vision

Several strengths and weaknesses of computational visual analysis clearly emerge from the application and results above, summarised in Figure 8 below.

*Figure 8. Strengths and weaknesses of computational visual analysis methods.*



Strengths

Big N

Fast

Invariable

Minimizes exposure

Zoomed-out

Theory-blind (unsupervised)

Struggles with multi-dimensionality

Weaknesses

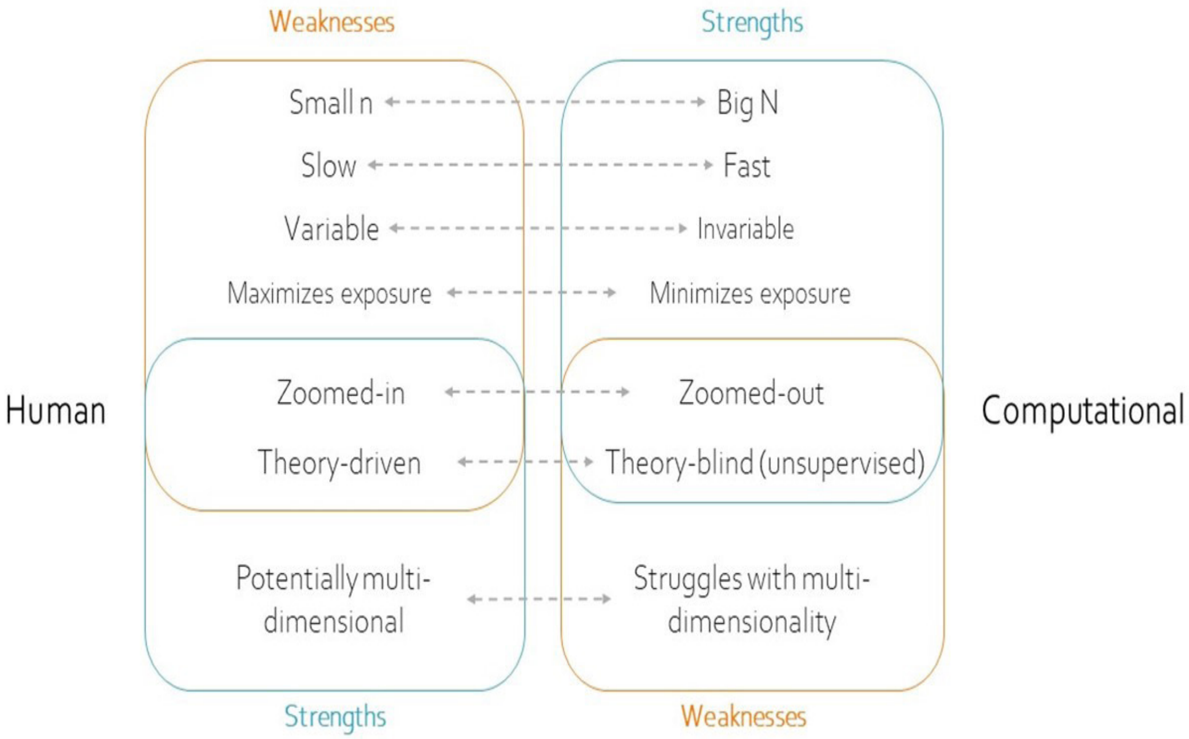
In terms of strengths, these methods are first and foremost capable of scaling-up the analysis to process huge visual corpora containing tens or hundreds of thousands of images, which is a critical asset in today's very large digital extremist environments. The bigger the corpus, the more useful these methods are, allowing the researcher to move from small-n samples to full corpus analysis, and to do so speedily, outpacing any human coder when it comes to detecting specific objects. In our case, we were able to rapidly detect images featuring specific classes of objects (i.e. Pepe, anime girls) from a large corpus. Importantly, these methods leverage transparent and replicable procedures invariably producing similar results on a given corpus (something never guaranteed with human methods). Finally, and not insignificantly, these automated methods also limits the researcher's exposure to potentially harmful material, which responds to the concerns recently voiced about one of the key challenges when handling terrorist and extremist images (cf. above).

Yet computational methods also have clear weaknesses. First, even though object detection models can identify several objects within the same image, computational methods still struggle with multi-dimensionality and latent meaning, lacking the human appreciation of how certain visual signifiers blend to create new composite signs, and still needing training to identify general visual classes expressed in many different forms (e.g. a "Nazi symbol"). Second, these methods are incapable of offering detailed qualitative interpretations of particularly important images or groups of images, as they only offer zoomed-out views of vast visual landscapes. Our clustering map, for instance, revealed the presence of large numbers of anime, and even grouped them into two distinct classes, but fell short of providing any real insight into what sub-variants may exist and, ultimately, what these images mean. These first two weaknesses are significant: In spite of their strengths, computational methods simply cannot do the type of in-depth work done in some of the aforementioned studies.[87] Third, the unsupervised models are theory-blind, which means that their purely inductive logic produces results that at times lack any usefulness and contain large residual categories – when they are not outwardly counter-productive. Clustering models sometimes need to be run several times with varying hyperparameters, both on the full corpus and within clusters, before they succeed in separating pictures into meaningful categories.

Yet the last two weaknesses also constitute strengths. First, the ability to offer zoomed-out perspectives on today's sprawling extremist digital ecosystems without pre-existing bias is critical, allowing the researcher to subsequently focus their efforts on the segments of the visual landscape that appear to dominate or matter in particular ways. Second, unsupervised methods' blindness to theory at times unlocks unexpected knowledge. As Grimmer, Roberts, and Stewart explain, hypothetic-deductive approaches force "researchers to use data to test theories that were developed before the data arrive", which "leaves potential insights on the table". By using inductive computational tools as a preliminary step, we "often discover new directions, questions, and measures", a step they call "quantitative discovery".[88]

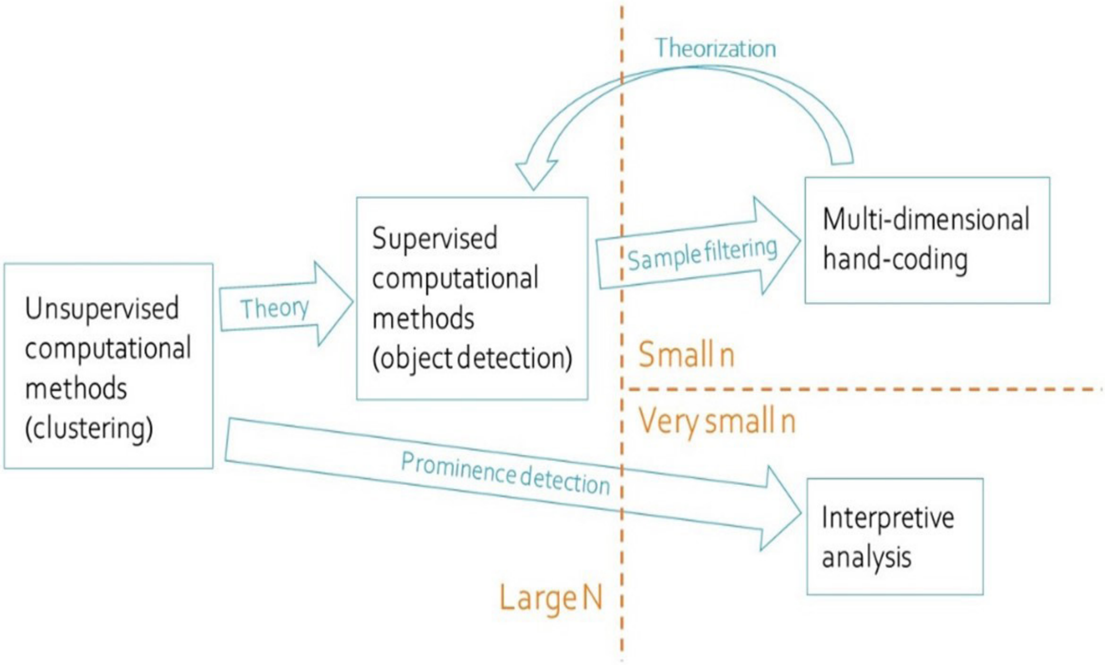
The reader has by now realised that the strengths and weaknesses of human versus computational methods mirror one another. Figure 9 below connects Figures 1 and 8 in a single graph, showing how one approach's strengths reflect the other's weaknesses. Such a conceptualisation naturally calls for human-computational mixed methods in extremism and terrorism studies, for the potential of the fields' "visual turn" to be fully realised. This proposition provides an operational response to Rodermond and Weerman's recent observation that in terrorism and extremism studies "each method has its own strengths and shortcomings, and each method has its particular problems when applied in practice."[89] Furthermore, we hope that our illustrative incel case-study has shown that in spite of its underlying technicality, productive computer vision necessarily involves "qualitative" fine-tuning, mobilising expert substantive knowledge – in that sense, the boundary between human and computational approaches is not an impermeable one.

*Figure 9. Strengths and weaknesses of human vs. computational visual analysis methods.*



We therefore propose to interlock both approaches into a single, coherent research workflow for the study of large extremist visual landscapes, as summarised in our final Figure 10 below. As Grimmer and Stewart rightly argued, "rather than replace humans, computers amplify human abilities," meaning that a dichotomous, quantitative-qualitative (human-computational) methodological opposition is misleading.[90] Our workflow starts by running a clustering model with different parameters, allowing us to explore the corpus without bias and gain a bird's eye perspective. This zoomed-out view can direct towards two scenarios, either allowing for the direct detection of prominent or important visual tropes to then be interpreted qualitatively or to help identify or refine relevant theory to calibrate an object detection model. To take our incel case, the clustering model revealed large clusters of human faces and bodies, which could serve as a basis to train an object detection model seeking to differentiate between particular, theoretically relevant types (e.g., types of men such as "chads" and "incels", or pictures featuring violence against women). These classes of images can thereafter serve as samples for a classic multi-dimensional hand-coding of a smaller sample (e.g., a codebook-based analysis of pictures featuring violence against women), whose results could, in turn, serve to re-calibrate a computer vision model to find more theoretically relevant sub-classes. As such, our workflow advocates the same logic articulated by Grimmer, Roberts, and Stewart in their reflection on computational text analysis methods: it deconstructs and revisits the deductive-inductive and quantitative-qualitative oppositions that too often paralyse progress in social sciences,[91] adopting a dynamic stream where iterative loops ensure that data, observation, expertise, and theory enrich each other. As Bucy and Joo note, fostering such a dialogue across deeply-entrenched traditions and academic training lines is a challenge,[92] but examples of good practice are starting to emerge; Crawford, Keen, and Suarez-Tangil, for instance, ran a clustering model on tens of thousands of images from various Chan image-boards to enrich theory and hone in a qualitative analysis of violent far-right memes.

*Figure 10. A research workflow for visual research in extremism and terrorism studies.*


Theorization
Unsupervised computational methods (clustering)
Theory
Supervised computational methods (object detection)
Sample filtering
Multi-dimensional hand-coding
Small n
Very small n
Prominence detection
Interpretive analysis
Large N

## Conclusion and Discussion: Towards Mixed Human-Computer Research Streams

The proliferation of online extremist content and digital terrorism-related communications has encouraged researchers to turn to social data science, and advances in artificial intelligence have further bolstered their use of computational methods. However, this effort has, so far, largely stayed within the confines of text and meta-data analysis, failing to unlock new horizons for the field's recent "visual turn." The present paper sought to affect this connection between computational and visual analysis by detailing how supervised and unsupervised computer vision models can enrich the study of extremist and terrorist imagery in decisive ways. We applied two of these models to an original corpus to explain and illustrate the strengths and weaknesses of computational visual analysis applied to extremism and terrorism research; because these benefits and limitations mirror those of human visual methods. We proposed a research workflow combining the two types of approaches and undermining the sterile qualitative-quantitative opposition too often preventing security studies to meet its potential.

Research on terrorist and extremist communications has greatly benefited from computational text analysis, which has effectively complemented qualitative methodologies; there is no reason why our "visual turn" shouldn't follow track. It is worth stressing, however, that this workflow doesn't exhaust the range of research questions and, therefore, methodological approaches and research agendas centring around extremist and terrorist imagery; as Bouko rightly emphasised, the plurality of visual dynamics constituting political reality call for an array of research questions and associated methods, some of them not even interested in the content of images (focusing, for instance, on impacts).[93]

It is hoped that our workflow and underpinning discussion will contribute to further materialise the recent optimistic assessments of our field's growing methodological strength,[94] which contrasts with the older, well-known negative and dire diagnoses of poor rigour, "failings", and "stagnation."[95] Specifically, adding computer vision to our methodological toolkit has the potential to partly correct terrorism studies' overreliance on qualitative designs (which make up more than three quarters of published research) and to move scholarship standards towards a more thorough and systematic exposition and justification of their methods (which is not done in most published articles).[96]

An integrated mixed-methods designs making the most of human and computational visual methods while mitigating each one's shortcomings not only makes scientific sense, it can also serve a positive social purpose at a time when visual AI models start to be leveraged by extremist and terrorist actors themselves (as well as by governments, in a dialectical power struggle).[97] As Bucy and Joo rightly suggest, "understanding the prevalence of these visual forms of hate, and accurately assessing their presence [...] could put visual politics to a prosocial use."[98] Beyond academia, law enforcement and security practitioners have started to leverage computational techniques to respond to "the urgent need to collect and analyze terrorist and extremist content online, on a large scale",[99] but often lack the tools to do so when it comes to imagery. Image clustering models can be run to rapidly situate the ideology and culture of an online space that has recently been brought to attention (for example, as part of an investigation or after an attack), while object detection models can be trained to look for specific details such as weapons (weapons visual datasets already exist that can feed the training), ideological markers such as svastikas, faces of individuals such as extremist leaders or potential attack targets (e.g. political figures), or high-risk content such as bomb-making blueprints. However, given the high stakes of this type of monitoring and analysis, law-enforcement and intelligence practitioners should be careful about the multiple errors, risks, and biases paving the approach, collection, and analysis of big data, which are by now well-documented.[100]

Finally, while primarily methodological, the contribution of this paper is also empirical. Using a real corpus as an illustrative example has incidentally led us to offer novel observations on the visual style of the incelosphere – which had, to our knowledge and surprise, not yet been systematically and directly studied.[101] Paving the way for a more comprehensive and in-depth study of incel imagery, we can already highlight the following three observations. First, the incel visual style appears to be highly composite and diverse, quite far from the typically narrow extremist landscapes featuring ingroup and outgroup archetypes (cf. above); a lot of the dataset is made of images that cannot easily be categorised into known theoretical categories. Second, most of the images feature specific individuals (actors, popular internet personalities, politicians, etc.) who have no obvious connection to the incel community; further research would need to adapt their methods to make sense of this fact. Finally, our dataset (unsurprisingly) contains a significant number of erotic or pornographic pictures and anime. Further research could examine the gender and sexual meanings of these images, which, among others, appear to ridicule women and picture them in submissive situations (in pictures) while simultaneously construct an idealised "girlfriend" stereotype (in anime), a paradox already highlighted in the text-based literature.[102]

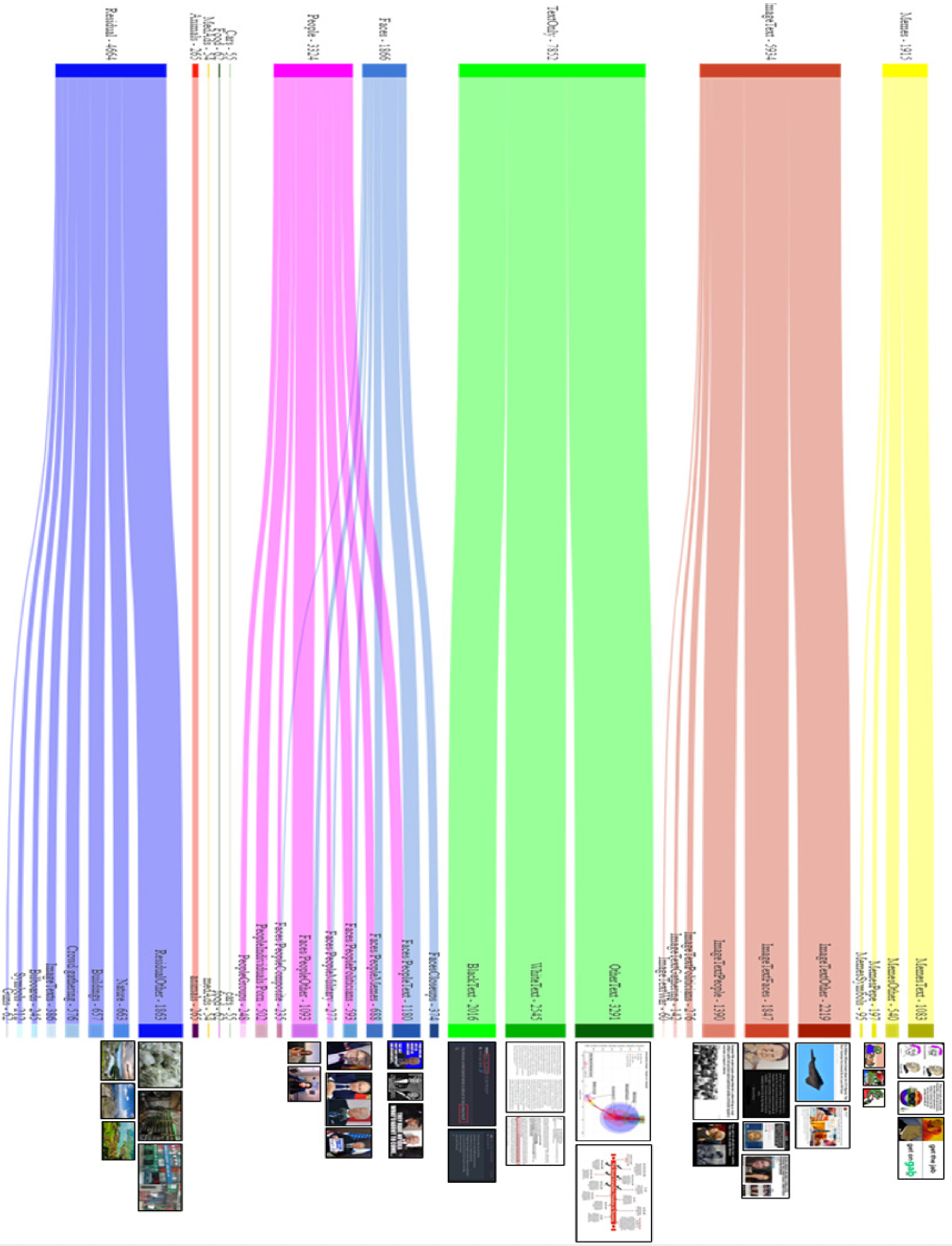
*Stephane J. Baele is Professor of International Relations at the University of Louvain (Belgium), and Honorary Associate Professor of Security and Political Violence at the University of Exeter (UK). His multidisciplinary work focuses on extremist and violent political actors' communications. On Twitter at @StephaneBaele.*

*Lewys Brace is Senior Lecturer in Computational Social Science at the University of Exeter (UK), where he is the co-Director of the Centre for Computational Social Sciences (C2S2). His work leverages data science and OSINT methods to study phenomena pertaining to terrorism, radicalisation, and cybercrime. On Twitter at @Lew_Brace.*

*Elahe Naserian is a senior AI engineer and data scientist at Trilateral Research UK, which she joined after a PhD at the University of West of Scotland and postdoctoral fellowships at the University of Exeter. She specialises in the development and application of Artificial Intelligence to analyse social issues.*

# Appendix 1: Far-Right Telegraph Clustering

*Figure A-1. Clustering diagram of images from the US Far-right Telegram ecosystem.*



# Appendix 2: Validation Metrics

Many of the metrics used to assess object detection models require understanding the difference between the “ground truth bounding box”, the bounding box that indicates the location of a specific class instance that was labelled by researchers, and the “predicted bounding box”, which is the bounding box that the algorithm believes contains a class instance. The “Intersection over Union” (IoU) is then a quantitive measure of the overlap between the two and can range between 0 (no overlap) and 1 (perfect overlap), with a higher IoU indicating more accurate object detection.

Each detection instance can then have one of three outcomes. First, it can be “true positive”, meaning the model correctly identified both the category and location of the object in an image and the IoU score is equal to or greater than the specific threshold. Second, the instance can be “false positive”, whereby the model incorrectly identifies an object that does not exist in the ground truth box or where the predicted bounding box has an IoU lower than the specific threshold. Finally, “false negative” refers to instances whereby the model failed to detect an object that is specific by the ground truth box.

One of the most important metrics when validating an object detection model is then the average precision (AP) score. Here, “precision” refers to how precise the model is, and it is essentially the proportion between the number of true positives and the number of predictions. Linked to this is the notion of “recall”, which is the ratio between the true positives the model makes and the number of ground truths; in other words, how many instances of an object in an image the model detects. More formally:

$$Precision = \frac{true\ positives}{true\ positives + false\ positives}$$

$$Recall = \frac{true\ positives}{true\ positives + false\ negatives}$$

# Endnotes

[1] On extremists and terrorists' technological innovation, read for example Adam Dolnik, *Understanding Terrorist Innovation. Technology, Tactics and Global Trends* (New York: Routledge, 2007); Yannick Veilleux-Lepage, *How Terror Evolves. The Emergence and Spread of Terrorist Techniques* (Lanham: Rowman & Littlefield, 2020).

[2] For a historical account, read Maura Conway, Ryan Scrivens, and Logan Macnair, "Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends," *ICCT Policy Briefs* (2019). For a panorama and theorization of the contemporary ecosystem, read Stephane Baele, Lewys Brace, and Travis Coan, "Uncovering the Far-Right Online Ecosystem: An Analytical Framework and Research Agenda," *Studies in Conflict & Terrorism* 46, no.9 (2020): 1599-1623.

[3] For a comprehensive account, see Stephane Baele, Katharine Boyd, and Travis Coan (eds.), *ISIS Propaganda. A Full-Spectrum Extremist Message* (New York: Oxford University Press, 2020).

[4] J.M. Berger and Jonathon Morgan, "The ISIS Twitter Census. Defining and Describing the Population of ISIS Supporters on Twitter," *Brookings Project on U.S. Relations with the Islamic World Analysis Papers* 20 (2015). See also Adam Badawy and Emilio Ferrara, "The rise of Jihadist Propaganda on Social Networks," *Journal of Computational Social Science* 1, no.2 (2018): 453-470; or Jytte Klausen, "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq," *Studies in Conflict & Terrorism* 38, no.1 (2015): 1-22.

[5] Manoel Horta Ribeiro, Jeremy Blackburn, Barry Bradlyn, Emiliano De Cristofaro, Gianluca Stringhini, Summer Long, Stephanie Greenberg, and Savvas Zannettou, "The Evolution of the Manosphere Across the Web," *Proceedings of the International AAAI Conference on Web and Social Media* 15, no.1 (2021): 196-207.

[6] Xinyi Zhang, and Mark Davis, "E-extremism: A conceptual framework for studying the online far right," *New Media & Society* 26, no.5 (2022).

[7] Justin Grimmer, Margaret Roberts, and Brandon Stewart, "Machine Learning for Social Sciences: An Agnostic Approach," *Annual Review of Political Science* 24 (2021): 395-396.

[8] See for example Manuela Caiani and Claudius Wagemann, "Online Networks of the Italian and German Extreme Right," *Information, Communication & Society* 12, no.1 (2009): 66-109; Caterina Froio and Bharat Ganesh, "The Transnationalisation of Far Right Discourse on Twitter," *European Societies* 21, no.4 (2019): 513-539; Ofra Klein and Jasper Muis, "Online Discontent: Comparing Western European Far-right Groups on Facebook," *European Societies* 21, no.4 (2019): 540-562; Aleksandra Urman and Stefan Katz, "What They Do in the Shadows: Examining the Far-right Networks on Telegram," *Information, Communication & Society* (2020), online before print.

[9] For example Ryan Scrivens, "Exploring Radical Right-Wing Posting Behaviors Online," *Deviant Behavior* 42, no.11 (2020): 1470-1484; Stephane Baele, Lewys Brace, Travis Coan, and Elahe Naserian, "Super- (and hyper-) posters on extremist forums," *Journal of Policing, Intelligence & Counter Terrorism* 18, no.3 (2023): 243-281.

[10] See for example Sylvia Jaki, Tom De Smedt, Maja Gwóźdź, Rudresh Panchal, Alexander Rossa, and Guy De Pauw, "Online Hatred of Women in the Incels.me Forum. Linguistic Analysis and Automatic Detection," *Journal of Language Aggression and Conflict* 7, no.2 (2019): 240-268; Ryan Scrivens, Garth Davies, and Richard Frank, "Measuring the Evolution of Radical Right-Wing Posting Behaviors Online," *Deviant Behavior* 41, no.2 (2020): 216-232; or Stephane Baele, Lewys Brace, and Debbie Ging, "A Diachronic Cross-Platforms Analysis of Violent Extremist Language in the Incel Online Ecosystem," *Terrorism & Political Violence* (2023), online before print.

[11] Stuart Macdonald, Elizabeth Pearson, Ryan Scrivens, and Joe Whittaker, "Using online data in terrorism research," In *A Research Agenda for Terrorism Studies*, edited by Lara Frumkin, John Morrison, and Andrew Silke (Edward Elgar, 2023): 145-158. Miriam Fernandez and Harith Alani, "Artificial Intelligence and Online Extremism. Challenges and Opportunities," In *Predictive Policing and Artificial Intelligence*, edited by John McDaniel and Ken Pease (London: Routledge, 2021).

[12] To our knowledge, there is no comprehensive, specific handbook of methods in terrorism research, but the broader terrorism studies handbooks that include methods sections do not feature visual approaches – see for example Erica Chenoweth, Richard English, Andreas Gofas, and Stathis Kalyvas, *The Oxford Handbook of Terrorism* (Oxford: Oxford University Press, 2019). Dixit and Stump's methods handbook stands out, but it solely includes "critical" approaches and its last chapter on visuals consists in an interview focusing only on visual representations of war on terror – see Priya Dixit and Jacob Stump, *Critical Methods in Terrorism Studies* (London: Routledge, 2016).

[13] See for instance David McNabb, *Research Methods for Political Science. Quantitative and Qualitative Methods. 2nd Edition* (New York: Routledge, 2015).

[14] By that we mean approaches that rely on the "hand" coding of limited samples of pictures (typically

between 100 and 1,000) by experts, and descriptive statistics built from this coding.

15 Stephane Baele and Charlie Winter, "From Music to Books, from Pictures to Numbers: The Forgotten Yet Crucial Components of Islamic State's Propaganda," In *ISIS Propaganda: A Full-spectrum Extremist Message*, edited by Stephane Baele, Katharine Boyd, and Travis Coan (New York: Oxford University Press, 2019): 188-218.

16 Stephane Baele and Lewys Brace, "AI Extremism. Technology, Tactics, Actors," *VoxPol Reports* (2024), https://voxpol.eu/file/ai-extremism-technology-tactics-actors/

17 Justin Grimmer and Brandon Stewart, "Text as Data: The Promise and Pitfalls of Automatic Content Analysis Methods for Political Texts," *Political Analysis* 21, no.3 (2013): 267-297.

18 Jungseock Joo and Zachary Steinert-Threlkeld, "Image as Data: Automated Content Analysis for Visual Presentations of Political Actors and Events," *Computational Communication Research* 4, no.1 (2022): 11-67.

19 Joo and Steinert-Threlkeld, "Image as Data," 35.

20 One important reason explaining the delayed adoption of computational visual methods within extremism research is indeed the lack of adequate resources available to researchers; using some of the supervised methods discussed below, for instance, has traditionally required lots of time dedicated to labelling the dataset for training.

21 See for instance Dan Schill, "The Visual Image and the Political Image: A Review of Visual Communication Research in the Field of Political Communication," *Review of Communication* 12, no.2 (2012): 118-142; Anastasia Veneti, Daniel Jackson, and Darren G. Lilleker (eds.), *Visual Political Communication* (Cham: Palgrave Macmillan – Springer, 2019)

22 For example Roland Bleiker, "The Aesthetic Turn in International Political Theory," *Millennium: Journal of International Studies* 30, no.3 (2001): 509-533; Roland Bleiker (ed.), *Visual Global Politics* (New York: Routledge, 2018); or Lene Hansen, "Theorizing the Image for Security Studies: Visual Securitization and the Muhammad Cartoon Crisis," *European Journal of International Relations* 17, no.1 (2011): 51-74.

23 Erik Bucy and Jungseock Joo, "Editors' Introduction: Visual Politics, Grand Collaborative Programs, and the Opportunity to Think Big," *The International Journal of Press/Politics* 26, no.1 (2021): 5-21.

24 Winkler and Dauber, *Visual Propaganda*, 13

25 Robin Engstrom, "The Online Visual Group Formation of the Far Right: A Cognitive-Historical Case Study of the British National Party," *Public Journal of Semiotics* 6, no.1 (2014): 1-21.

26 Neville Bolt, *The Violent Image: Insurgent Propaganda and the New Revolutionaries* (New York: Columbia University Press, 2012).

27 Nicole Doerr, Alice Mattoni, and Simon Teune, "Toward a Visual Analysis of Social Movements, Conflict, and Political Mobilization," *Research in Social Movements, Conflicts and Change* 35 (2013).

28 Caroline Winkler and Cori Dauber (eds.), *Visual Propaganda and Extremism in the Online Environment* (Carlisle, PA: US Army War College Press, 2014).

29 Maura Conway, "We Need a 'Visual Turn' in Violent Online Extremism Research," *VoxPol Blog* (2019), available at https://www.voxpol.eu/we-need-a-visual-turn-in-violent-online-extremism-research/.

30 Jens Seiffert-Brockmann, Trevor Diehl, and Leonhard Dobusch, "Memes as Games: The Evolution of a Digital Discourse Online," *New Media & Society* 20 (2018), no.8: 2862-2879.

31 Scrivens, Freilich, Chermak, and Frank, "Data Collection".

32 Stephane Baele, Katharine Boyd, and Travis Coan, "Lethal Images: Analyzing Extremist Visual Propaganda from ISIS and Beyond," *Journal of Global Security Studies* 5, no.4 (2019): 634-657

33 Stephane Baele, Katharine Boyd, and Travis Coan, "Lethal Images."

34 Charlie Winter, *The Terrorist Image. Decoding the Islamic State's Photo-Propaganda* (New York: Hurst, 2022).

35 Stuart Macdonald and Nuria Lorenzo-Dus, "Visual Jihad: Constructing the "Good Muslim" in Online Jihadist Magazines," *Studies in Conflict & Terrorism* 44, no.5 (2021): 363-386.

36 Sarah Awad, Nicole Doerr, and Anita Nissen, "Far-right Boundary Construction Towards the "Other": Visual Communication of Danish People's Party on Social Media," *British Journal of Sociology* 73, no.5 (2022): 985-1005.

37 Catherine Tebaldi, "Granola Nazis and the Great Reset. Enregistering, Circulating and Regimenting

Nature on the Far Right," *Language, Culture & Society* 5 (2023), no.1: 9-42.

38 Tebaldi, "Granola Nazis".

39 Engstrom, "The Online Visual Group Formation of the Far Right," p.2.

40 Tebaldi, "Granola Nazis".

41 Drew Halfmann and Michael Young, "War Pictures: The Grotesque as a Mobilizing Tactic," *Mobilization: An International Quarterly* 15, no.1 (2010): 1-24

42 Carol Winkler, Kareem El Damanhoury, Aaron Dicker, and Anthony Lemieux, "The Medium is Terrorism: Transformation of the About to Die Trope in Dabiq," *Terrorism & Political Violence* 31, no.2 (2019): 224-243.

43 Lilie Chouliaraki and Angelos Kissas, "The Communication of Horrorism: A Typology of ISIS Online Death Videos," *Critical Studies in Media Communication* 35, no.1 (2018): 24-39.

44 These are often interpreted as "projectilic" images, to use the concept developed by Marwan Kraidy, "The Projectilic Image: Islamic State's Digital Visual Warfare and Global Networked Affect," *Media, Culture & Society* 39, no.8 (2017): 1194-1209.

45 Nicole Doerr, "Bridging Language Barriers, Bonding Against Immigrants: A Visual Case Study of Transnational Network Publics Created by Far-right Activists in Europe," *Discourse & Society* 28, no.1 (2017): 3-23.

46 Nicole Doerr and Beth Gharrity Gardner, "After the Storm. Translating the US Capitol Storming in Germany's Right-wing Digital Media Ecosystem," *Translation in Society* 1, no.1 (2022): 83-104.

47 Nicolò Miotto, "Visual Representation of Martyrdom: Comparing the Symbolism of Jihadi and Far-right Online Martyrologies," *Journal for Deradicalization* 32 (2022): 110-163.

48 Julia DeCook, "Memes and Symbolic Violence: #Proudboys and the Use of Memes for Propaganda and the Construction of Collective Identity," *Learning, Media & Technology* 43 (2018), no.4: 485-504.

49 Roland Bleiker, "Pluralist Methods for Visual Global Politics," *Millennium: Journal of International Studies* 43, no.3 (2015): 872-890.

50 Engstrom, "The Online Visual Group Formation of the Far Right."

51 For instance, Hendry and Lemieux's study of Atomwaffen Division videos only operationalized 12 straightforward categories such as "key symbols", "flag", "infrastructure", or "militant". John Hendry and Anthony Lemieux, "The Visual and Rhetorical Styles of Atomwaffen Division and their Implications," *Dynamics of Asymmetric Conflict* 14, no.2 (2021): 138-159.

52 Jungseock Joo and Zachary Steinert-Threlkeld, "Image as Data," p.12.

53 See Elizabeth Pearson, Joe Whittaker, Till Baaken, Sara Zeiger, Farangiz Atamuradova, and Maura Conway, "Online Extremism and Terrorism Researchers' Security, Safety, and Resilience: Findings from the Field," *VoxPol Reports* (2023).

54 Roderick Hart, "Redeveloping DICTION: Theoretical Considerations," in *Theory, Method and Practice in Computer Content Analysis*, edited by Mark West (New-York: Ablex, 2001): 43–60.

55 Ekaterina Zagarniuk, "What is Computer Vision?" *Medium*, 24 February 2022, https://medium.com/@zagarnyuk.ek/what-is-computer-vision-10c7027e867. This article provides a clear overview of how computer vision works and its main applications.

56 Joo & Steinert-Threlkeld 2022: 17.

57 *ImageNet* accurately classified over a million photos from a challenge corpus into 1000 distinct classes ("leopards", "mushrooms", "pumpkins", "container ships", etc.). See Alex Krizhevsky, Ilya Sutskever, and Geoffrey Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," *Advances in Neural Information Processing Systems* 25, no.2 (2012).

58 See Mario Haim, Marc Jungblut, "Politicians' Self-depiction and their News Portrayal: Evidence from 28 Countries Using Visual Computational Analysis," *Political Communication* (2020), online before print; Amogh Joshi and Cody Buntain, "Examining Similar and Ideologically Correlated Imagery in Online Political Communication," *arXiv* 2110.01183v2 (2022).

59 Yilang Peng, "What Makes Politicians' Instagram Posts Popular? Analysing Social Media Strategies of Candidates and Office Holders with Computer Vision," *International Journal of Press/Politics* 26, no.1 (2021): 143-166.

60 Theisen and colleagues for example offered a method that "ingest images from a social network, apply computer vision-based techniques to extract local features and index new images into a database,

and then organize the memes into related genres" (p.714), and used this method to study over 2 million images circulated on Twitter and Instagram during the 2019 Indonesian presidential elections. See William Theisen, Joel Brogan, Pamela Thomas, Daniel Moreira, Pascal Phoa, Tim Weninger, and Walter Scheirer, "Automatic Discovery of Political Meme Genres with Diverse Appearances," *Proceedings of the International AAAI Conference on Web and Social Media* 15, no.1 (2021): 714-726.

[61] Joel Finkelstein, Savvas Zannettou, Barry Bradlyn and Jeremy Blackburn, "A Quantitative Approach to Understanding Online Antisemitism," *arXiv* 1809.01644v1 (2018).

[62] Blyth Crawford, Florence Keen, and Guillermo Suarez-Tangil, "Memes, Radicalization, and the Promotion of Violence on Chan Sites," *Proceedings of the Fifteenth International AAAI Conference on Web and Social Media (ICWSM )* (2021): 982-991.

[63] Kay O'Halloran, Sabine Tan, Peter Wignell, John Bateman, Duc-Son Pham, Michele Grossman and Andrew Vande Moere, "Interpreting Text and Image relations in Violent Extremist Discourse: A Mixed-Methods Approach for Big Data Analytics," *Terrorism & Political Violence* 31, no.3 (2019): 454-474.

[64] These online spaces were identified through both extensive exploration of incel online spaces and snowball sampling and were selected based on both their content and their use of images in posts.

[65] Bum Chul Kwon, Ben Eysenbach, Janu Verma, Kenney Ng, Christopher De Filippi, Walter F. Stewart, and Adam Perer Kwon, "Clustervision: Visual Supervision of Unsupervised Clustering," *IEEE Transactions on Visualization & Computer Graphics* 24, no.1 (2018): 142-151.

[66] Grimmer, Roberts and Stewart, "Machine Learning for Social Sciences," p.407.

[67] Sungwon Park, Sungwon Han, Sundong Kim, Danu Kim, Sungkyu Park, Seunghoon Hong, and Meeyoung Cha, "Improving Unsupervised Image Clustering With Robust Learning," *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (2021): 12278-12287. For a recent tutorial see https://medium.com/@info.martinanto/yolov3-for-weapon-detection-artificial-intelligence-dialling-911-6a4b47ba637c.

[68] Grimmer and Stewart, "Text as Data," 280.

[69] Grimmer and Stewart, "Text as Data," 281.

[70] Joshi and Buntain, "Examining Similar and Ideologically Correlated Imagery," 10.

[71] Junyuan Xie, Ross Girshick, Ali Farhadi, "Unsupervised Deep Embedding for Clustering Analysis," *Proceedings of the 33rd International Conference on Machine Learning* (2016).

[72] An important point not just because of the aforementioned overfitting issue, but also because of the computational time required to run such models for more epochs.

[73] Richard Rogers, "Visual Media Analysis for Instagram and Other Online Platforms," *Big Data & Society* 8, no.1 (2021).

[74] The far-right cluster map provided in Appendix 1 is less directly informative because the algorithm had trouble sorting the main type of visual imagery present on the Telegram channels: text-image combinations. Discounting the text-only pictures, far-right Telegram channels appear to heavily picture photos of individuals (Trump, Biden, other US politicians, US military officers, far-right influencers, Nazi leaders, etc.).

[75] Similarly, the far-right cluster map in Appendix 1 groups together images of politicians in formal settings (typically wearing suits in front of flags), but gives no indication as to who these individuals are or when members share this type of photographs. The same applies to the cluster grouping faces with texts: it bundles together evidently distinct categories of people (e.g. Nazi Germany officials, US politicians) but is unable to clarify what these categories are and what kinds of text (motivational, defamatory, etc.) accompany them to form multimodal meaning.

[76] Zhengxia Zou, Keyan Chen, Zhenwei Shi, Yuhong Guo, and Jieping Ye, "Object Detection in 20 Years: A Survey," *Proceedings of the IEEE* 111, no.3 (2023): 257-276.

[77] F. Sultana, A. Sufian, P. Dutta, "A Review of Object Detection Models Based on Convolutional Neural Network," in: *Intelligent Computing: Image Processing Based Applications,* ed. J. Mandal and S. Banerjee, vol. 1157, *Advances in Intelligent Systems and Computing* (Singapore: Springer, 2020). This review and the one cited in the previous endnote offer excellent explanations of how object detection models work, information on the differences between them, and overviews of their steady improvement over the past decade.

[78] Zou and colleagues, "Object Detection in 20 Years," p.257.

[79] Zou and colleagues, "Object Detection in 20 Years," p.259

[80] See for example Sanam Narejo, Bishwajeet Pandey, Doris Esenarro Vargas, Ciro Rodriguez, and Anjum Rizwan, "Weapon Detection Using YOLO V3 for Smart Surveillance System," *Mathematical Problems in Engineering* (2021), doi:10.1155/2021/9975700.

[81] Joseph Redmon, Santosh Divvala, Ross Girshick, and Ali Farhadi Redmon, "You Only Look Once: Unified, Real-Time Object Detection," *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (2016): 779-788.

[82] The authors would like to thank the team behind https://www.makesense.ai/, which was used for this task.

The authors would like to extend their thanks to the developers of Ultralytics (https://docs.ultralytics.com/) for their work on these open-source YOLO models.

[83] The developers of the COCO dataset, which is the widely adopted benchmark dataset used within the computer vision research and development community, have outlined the issues and extensive work needed to develop such a large data consisting of 2.5 million labelled instances across 328, 000 images; see Tsung-Yi Lin, Michael Maire, Serge Belongie, Lubomir Bourdev, Ross Girshick, James Hays, Pietro Perona, Deva Ramanan, C. Lawrence Zitnick, Piotr Dollar, "Microsoft COCO: Common Objects in Context," *Proceedings of the 13th European Conference on Computer Vision (ECCV)* (2014).

[84] The reason behind this low cut-off value was to yield a training dataset that would simply demonstrate how the YOLO model behaves with different numbers of instances for different classes.

[85] See https://docs.ultralytics.com/.

[86] The pornographic images have been blurred with a white square.

[87] For example Engstrom, "The Online Visual Group Formation of the Far Right," or Miotto, "Visual Representation of Martyrdom".

[88] Grimmer, Roberts and Stewart, "Machine Learning for Social Sciences," 404.

[89] Elanie Rodermond and Frank Weerman, "The Strengths and Struggles of Different Methods of Research on Radicalization, Extremism, and Terrorism," *Studies in Conflict & Terrorism* (2024), online before print: 1.

[90] Grimmer and Stewart, "Text as Data," 270.

[91] Grimmer, Roberts and Stewart, "Machine Learning for Social Sciences," 403.

[92] Bucy and Joo, "Editors' Introduction."

[93] Catherine Bouko, *Visual Citizenship. Communicating Political Opinions and Emotions on Social Media* (London: Routledge, 2023).

[94] For example Rodermond and Weerman, "Strengths and Struggles," or Bart Schuurman, "Research on Terrorism, 2007–2016: A Review of Data, Methods, and Authorship," *Terrorism & Political Violence* 32, no. 5 (2020): 1011-26.

[95] For a review of these assessments, see Schuurman, "Research on Terrorism, 2007–2016."

[96] These two observations are documented in Schuurman, "Research on Terrorism, 2007–2016."

[97] Baele and Brace, "AI Extremism."

[98] Bucy and Joo, "Editors' Introduction."

[99] Ryan Scrivens, Joshua Freilich, Steven Chermak, and Richard Frank, "Data Collection in Online Terrorism and Extremism Research: Strengths, Limitations, and Future Directions," Studies in Conflict & Terrorism (2024), online before print: 1-23.

[100] Fernandez and Alani, "Artificial Intelligence and Online Extremism," Read also Alexandra Olteanu, Carlos Castillo, Fernando Diaz, and Emre Kıcıman, "Social Data: Biases, Methodological Pitfalls, and Ethical Boundaries," *Frontiers in Big Data* 2, no.13 (2019).

[101] All publications offering analysis of incel online content include text but not images, and several have called for this blind spot to be corrected. For example, we read an encouragement to conduct "a study of visual tropes reflecting an endorsement of violent extremism, such as avatar profiles containing pictures of killers or nazi iconography" in Stephane Baele, Lewys Brace, and Debbie Ging, "A Diachronic Cross-Platforms Analysis of Violent Extremist Language in the Incel Online Ecosystem," *Terrorism & Political Violence* 36 (2023), no.3: 382-405.

[102] Stephane Baele, Lewys Brace, and Travis Coan, "From 'Incel' to 'Saint': Analyzing the Violent Worl-

dview Behind the 2018 Toronto Attack," *Terrorism & Political Violence*, 33(2019), no.8: 1667-1691.

PT PERSPECTIVES ON TERRORISM

Research Article

# "I'm Not Super Familiar with Children's Ecosystems Online": Expert Assessments on the Effects of Early Childhood Exposure to Extremism Online

Jade Hutchinson,* David Yuzva Clement, Ruxandra M. Gheorghe, Lorraine Kellum, and Alexander Shuttleworth

Volume XIX, Issue 1
March 2025

ISSN: 2334-3745
DOI: 10.19165/2025.5669

**Abstract:** This article brings together expert assessments concerning the relationship between children and online extremism, to help inform scholars and policymakers seeking to address the effects of early childhood exposure to extremism content. Our approach comprised of eight semi-structured interviews involving experts, practitioners, and policymakers offering their professional assessments on the relationship between children and online extremist content. Findings include the role of online misogyny and its psychological appeal to children and adolescents in digital media environments, especially when viewed alongside or expressed in politically benign online spaces in the children's lifestyle or development. Results emphasised the evolving sociotechnical contexts where children are being exposed to extremist content, chiefly the rapid development in online gaming communities and allied innovation in gaming industries. The experts interviewed see interdisciplinary collaboration with health, cognitive-psychological, and neuro-developmental sciences specific to child development and psychology as essential for understanding the effects of online extremist content on children in future studies. Their recommendations centred on prioritising digital media literacy in schools, promoting community engagement and parental discussions about child safety online, incentivising companies responsible for products used by children to implement age verification and advanced moderation policies, and supporting localised culture figures in the children's lifestyle and development alongside social workers and childhood educators. Findings also suggest that current school systems and curricula lack comprehensive prevention or counter-measures against growing radicalisation in child settings. Participants offered ideas on addressing children's exposure to online extremist content, yet gaps remain in implementing effective strategies within educational settings and beyond.

**Keywords:** Extremism, online, children, policy, safety, social media, ideology, gaming

* *Corresponding author: Jade Hutchinson, Charles University (Czech Republic). E-mail: jade.hutchinson@mq.edu.au*

## Introduction

In recent years, children under the age of fourteen are spending ever more time with technologies like social media and online gaming platforms. Time spent using such technologies has significantly increased among international populations of young people (generally under eighteen years of age) since the beginning of the COVID-19 pandemic.[1] Emerging research continues to identify various psychological and academic implications associated with children's involvement in social media and online gaming communities.[2] Increased interconnectedness between children and the technologies used in extremist communities is anticipated to heighten the likelihood of children encountering extremist materials online – particularly among socially isolated children and teenagers who are more likely to exhibit technological over-reliance and ideologically problematic internet use.[3] Subsequently, recent studies have explored how extremist recruiters could leverage the convenience, connectivity, and anonymity of widely adopted digital media platforms to persuade or manipulate younger audiences. Children are currently being represented in violent extremist content, and those materials do appear in populations of children and adolescents through the democratisation of online gaming and social media technologies, surging victimhood or misogynistic sentiment in these spaces.[4] Empirical studies focused on the relationship between online extremism and children under fourteen years of age are rare, and, as a consequence, contemporary professional assessments and recommendations regarding early childhood exposure to extremism online are limited. Therefore, it is important to explore what professional assessments and policy recommendations are currently discussed among terrorism and extremism researchers and policy-makers, with the intent to offer guidance to future researchers and move policy initiatives forward.

## Current Study

This article brings together expert analyses and assessments concerning the relationship between children and online extremism, exploring the manifest ways that scholars, practitioners, and policymakers understand and hope to address the effects of online extremism on early childhood development. For the purpose of this study, we understood children as persons between seven and thirteen years of age, as this is a period of significant social and cognitive advances in childhood and when children begin to establish their sense of identity.[5] First, we explored the relevant literature circling childhood exposure to extreme ideological digital media (and where possible, "self-radicalisation" and online extremism in this context). Second, we interviewed eight experts on the effects of early childhood exposure to online extremism. Third, we bring together the policy and research recommendations from the data collected from our expert interviewees.

Findings highlight the prevalence and psychological appeal of online misogyny among children exploring digital media environments, with specialists emphasising insecure, frustrated, and marginalised boys as especially susceptible to mimicry.[6] Extreme online materials were considered increasingly present and linked to children and adolescents' favourite platforms and devices, with interviewees particularly concerned about their promotion of extreme – and at times undemocratic and regressive – offline conduct and ideologies for the purpose of obtaining social validation and appreciation from peers. Moreover, our study uncovered concerns about children's engagement with digital media technologies concerning the normalisation of online hatred and misogyny. This included misconceptions about how children routinely interact with and think about digital media technology when exposed to influential cultural figures, like Andrew Tate.[7, 8] Social cognitive theory provides additional context here, as it posits that children imitate behaviours they observe in influential media figures, especially if those figures appear rewarded for their actions.[9] Within these sociotechnical contexts, participants stressed the necessity to work collaboratively with private technology companies to develop monitoring and preventative measures specific to early childhood exposure. Furthermore, our research underscored the necessity for interdisciplinary collaboration and innovative research methodologies between terrorism and extremism studies and cognitive psychology to better understand the effects of early childhood exposure to online extremist materials. Finally, we bring together a set of policy and practice recommendations from our expert interviews, centring digital media literacy in schools, community and parental discussions about child online safety, incentivising companies responsible for products used by children to implement age verification and advanced moderation policies, and supporting localised figures in children's communities alongside child psychologists, social workers, and childcare workers. Elucidating the existing knowledge gaps, and research and policy-making challenges, this article contributes a series of professionally informed insights and recommendations to protect children from the influence of extremist materials online. However, it is important to emphasise that the policies and practices recommended are outcomes derived from our analysis of interview data and were directly informed by our findings. Such outcomes are intended to advance research concerning the nature of the relationship between younger users and extremism online, in addition to expanding the community of stakeholders through implementing guidelines and recommendations that address the realities of early childhood exposure. Notably, however, findings suggest that current school systems and curricula lack comprehensive prevention or counter-measures against growing exposure to extremist content in child settings.[10, 11]

## Literature Review

The emergence of social networking technologies, the development of online gaming communities, and the associated evolution of digital youth subcultures have created circumstances where children are more likely to encounter extremist materials.[12] Recent studies on the "pathways" of "online radicalisation" highlight the differences between patterns in online social behaviours in correspondence with advances in social networking technologies.[13] Terms like "organic" and "strategic" are progressively used to distinguish between digital media environments that stimulate young people to pursue or become incrementally receptive to online extremist materials, and whether digital media environments are deliberately or intentionally used as a "tool" for disseminating extremist messaging and engaging in recruitment. For instance, within the context of extremist content in online gaming communities, "organic gaming"[14] occurs when individuals involved in online gaming communities are exposed to or are influenced by extremist materials through gameplay interaction.[15] On the other hand, "strategic gaming" comprises a conscious effort to instrumentalise online gameplay, architectural designs, and digital media applications to disseminate ideologies and recruit audiences online. For example, customising content containing ideological messages and exploiting the games' communication systems to propagate and introduce custom-made materials in online gamer conversations is an example of strategic gaming.[16] Emerging research that has conceptualised organic and strategic approaches has importantly emphasised the dynamic and fluid interplay between gaming subcultures and problems surrounding identity fusion with radical ideologies, rather than simply problematising the game in and of itself.[17] Similarly, there seems to exist consensus that the Internet acts as a catalyst or facilitator, far less as a driving casual factor, for radicalisation.[18]

Social media and online gaming companies have also been identified as fostering a significant vulnerability for children exposed to extremist content through their use of "dark patterns."[19] Dark patterns refer to manipulation techniques employed by software developers to encourage prolonged engagement with their products. Examples of these tactics include countdown timers, hidden costs, "endless treadmill" mechanics, and low privacy settings, among many others.[20] These techniques are designed to exploit the limited ability of children to discern manipulative information, thereby "nudging" them to continue engaging in online activity for extended periods. In 2019, the United Kingdom enacted the "Age Appropriate Design Code", referred to as the "Children's Code", which established standards for online services to follow since its implementation in September 2021.[21] This code aims to enhance youth safety and protect data privacy by mandating differential data processing for users under the age of eighteen. Specific measures include the removal of auto-play features for children and default privacy settings on accounts that are used by those under the age of eighteen.[22] The Age Appropriate Design Code has had a global influence, prompting similar policy developments in Europe, Canada, Australia, and California.[23] However, compliance is not universal. For instance, TikTok faced accusations of permitting children under the age of thirteen to create user accounts without parental consent, extensively collecting their data, and refusing to delete this data upon request from the child or their family.[24] Overall, social media platforms offer different affordances and, therefore, facilitate radicalisation and extremism in differing ways.[25]

It is unclear the extent to which children are being intentionally recruited in online environments when compared to other age demographics, such as adolescents and young adults. Investigative news reporting related to this problem has speculated the role that influencers and technological platforms play in "radicalising" children. For example, a nine-year-old boy was supposedly recruited by his older brother, who introduced him to online "right-wing extremist" gaming communities.[26] Another case concerned two children aged nine and ten who had watched TikTok videos of influencer Andrew Tate and – as the report suggested – encouraged these children to demonstrate "toxic masculinity" in classrooms, such as victimising other children in the classroom, especially girls.[27] In the same reporting, teachers were interviewed and had expressed their insecurities concerning the increased presence of misogynistic behaviour and the behaviours' perceived implications for the children's worldview in early education, in addition to degrading the school's overall atmosphere and intergroup dynamics between genders.[28] In the United Kingdom, another report illustrated similar circumstances where children were officially referred to the Prevent programme, owing to their expressions of misogynistic behaviour in schools.[29]

Irrespective of news media publications reporting on this phenomenon, there remains a substantial empirical component missing in our examination of early childhood exposure to online extremist violence.[30] Certain countries are witnessing a decrease in the average age of those individuals who have observed violent extremist material online.[31] For example, Waldek and colleagues asked young adult Australians – aged eighteen to twenty-four years – their feelings and encounters with such content while online, highlighting how interviewees were exposed to the Christchurch far-right terrorist attack: either the full livestream or partial clips of the livestream footage in 2019.[32] A large-scale survey of 25,142 European children aged nine to sixteen revealed that exposure to pornography (21 percent) and violence (18 percent) were the most frequently reported online risks, with social networking sites and gaming platforms as the most common sources of exposure. Gaming platforms, in particular, were associated with violent content, which accounted for 39 percent of the risks identified within those spaces.[33] Anecdotal findings shared during a Radicalisation Awareness Network round-table conference similarly pointed to Dutch children who watched footage of the Christchurch attack and were exposed to racist online content on TikTok.[34] Furthermore, Rousseau and colleagues recently found that sympathy for violent radicalisation had decreased in age amongst high school students in Quebec (Canada).[35]

In tandem with other social networking technologies, networked online gaming communities – referred to as "online gaming ecosystems" – are increasingly identified as environments where young people can be dangerously exposed to online extremism.[36] Communities circling online gaming are considered particularly accessible, yet relatively opaque and semi-public spaces where children can – often unsupervised and at their convenience – create and manage private conversations and experience emotionally salient social encounters that are difficult to monitor or moderate externally.[37] Analogous to cyber grooming for sexual abuse (or "sextortion"), groomers purposefully narrowcast to potential recruits in online gaming communities, targeting vulnerable populations like children.[38] Recruiters identify specific groups of people to target their propaganda, and in the case of younger audiences, recruiters can tailor their messages by imitating youth cultural themes and aesthetics, including humour, meme culture, satire, as well as pessimism, normalising the content's extreme ideological undercurrents.[39] Targeting younger audiences is comparable to targeting older audiences as a developmental strategy for growing extremist communities and other criminal activities.[40]

It is worth remembering how the self-styled Islamic State of Iraq and Syria intentionally targeted young children and adolescents during their virtual propaganda campaigns. One central tactic was manufacturing adulterated gameplay footage from the videogame titled "Grand Theft Auto V" to appeal to children and adolescents.[41] Research indicates that certain religiously-motivated violent extremist groups and white supremacist groups have been producing extremist video games since the early-to-mid 2000s.[42] Combined with online gaming's interactive design, such technologies efficiently facilitate the socialisation between players and empower online extremist beliefs to germinate during gameplay. These recruiters regenerate game-based iconography and migrate between messaging applications, social media platforms, and online gaming platforms to build new recruit networks to communicate their ideologies amongst an increasingly younger viewership.[43] These dynamics can facilitate a technological milieu where connections are made, commitment can be demonstrated, grievances can be directly communicated and contended with, while children potentially develop "alternative identities" and extreme worldviews in response.[44]

For example, during an investigation of two male children aged twelve in Germany, Koehler and colleagues described how these children were groomed by online recruiters through gameplay, having publicly displayed right-wing extremist symbolism in their profiles on the online gaming platform Roblox.[45] The recruiters ushered the children into adjacent far-right Discord servers, where they were subjected to further ideological indoctrination, such as being exposed to anti-Semitic and neo-Nazi digital propaganda. The influence these handlers had on these children in establishing an emotional dependence was what the children likely experienced as "friendship" or "belonging".[46] Moreover, these children were too afraid to endanger their "bond" with their handlers, diligently following their groomers' instructions, such as performing the Hitler salute during school. The two children's cognitive openness was combined with the technologies' ability to facilitate their respective social and emotional integration with their recruiters, giving the children a sense of meaning and purpose. Furthermore, Koehler and colleagues noted that the children believed such social and psychological qualities were missing from their everyday lives, which were otherwise characterised by bullying and family conflicts.[47] This aligns with existing literature that documents the direct impact of social rejection on children's preference for antisocial and violent media.[48] This case highlights the significance of Valentini's "onlife" concept, where hybrid interactions between online and offline realities can lead to a continuum of behavioural adaptations owing to the child's indoctrination, like translating the groomer's online instructions into maladaptive actions (e.g. Hitler salute) in public spaces.[49]

Emerging research has further examined the dynamics of online radicalisation among children in school and household settings. Caton and Landman conducted a school-based study involving children (eleven to sixteen years old) with learning disabilities, parents or caregivers, and their teachers.[50] Although the children had a general understanding of the grooming process that facilitates online extremist recruitment efforts, their parents and teachers expressed concerns about the children's vulnerability to interacting with strangers in cyberspace, challenging their children's maturity and capacity to think critically when connecting with unknown persons in unsupervised settings. Additionally, parents and educators highlighted their own challenges to guarantee their children's safety. In a similar vein, Brisson-Boivin highlighted that youth intellectualise components or processes of online radicalisation when asked about these topics by adults or teachers, but youth are generally uncertain about how to respond to online extremist material or advances from recruitment when on their own.[51]

This is worrisome, considering surveys of children and young people have frequently demonstrated that youths are exposed to racism, hatred, and extremist ideology while in cyberspace. The German JIM study found 43 percent of all respondents aged twelve to nineteen experienced exposure to extreme political views, 43 percent were exposed to conspiracies, and 35 percent to hate messages while online.[52] In a pan-European study of nine-to-sixteen-year-olds (*n*=10,000), participants reported a range of risks that concern them on the internet.[53] The researchers found that pornography (22 percent), cyberbullying (19 percent), and violent content (18 percent) were at the top of young people's concerns.[54] Another survey of Canadian youths aged twelve to sixteen years old (*n*=1,000) found that while reporting encounters of extremism or hatred online was considered important, there remained a considerable proportion of participants that were hesitant to record reflections about their encounters with extremist materials online. Their reasons for not reporting encounters varied, such as fears of making the situation worse, having a scarce understanding of whether the content they were exposed to had warranted a report, and believing that reporting their online encounters will not effectively translate into actionable outcomes.[55] Nonetheless, the youth preferred two approaches to responding to online hate and extremism: (1) either stop communicating or prevent the producer from communicating (i.e. blocking) further online hate; and (2) engage their parents or caregivers about their experience.

Lastly, law enforcement agencies from Australia, Canada, New Zealand, the United Kingdom, and the United States have recently published a call for collective action, highlighting the vulnerability of minors towards radicalisation and recruitment by violent extremist and terrorist groups especially within online environments, discussing several country-specific case studies, and offering recommendations for a whole-of-society approach.[56] Collectively, these agencies stress the need for stronger multi-sectoral collaboration between law enforcement, security, government agencies, the education sector, mental health and social support services, communities, and technology companies to thwart youth radicalisation to violence while also highlighting support systems in the respective countries.

## Methods

To better understand the effects and possible preventative measures related to early childhood exposure to online extremist materials, this study conducted semi-structured interviews with experts, practitioners, and policy-makers (*n*=8). Interviews took place from July until September 2023, using a mix of deductive and open-ended questions, as well as probing and technical questions. Semi-structured interviews provided interviewees the freedom to express their experiences conducting research, producing policies, or practising in community settings, without restricting perspectives to a predetermined set of questions. All interview questions were shared with the interviewees prior to the meeting.

We used purposive sampling to invite eight experts from various sectors, including academia, frontline industries, practitioners in P/CVE organisations, and government agencies. Together, interviewees from Australia, Canada, Germany, the Netherlands, and the United Kingdom were included in this study. Informed consent was obtained prior to meeting each interviewee. All interviews were conducted and video- and audio-recorded via Zoom Video Communications. Interviews occurred for approximately 45 to 90 minutes. Interview transcripts were anonymised and transcribed verbatim using NVivo transcription software. Pseudonyms were used to de-identify the data and maintain confidentiality. Data analysis followed Braun and Clarke's six steps to reflexive thematic analysis, with codes developed in relation to the research questions, resulting in the identification of overarching themes, iteratively informing subsequent interviews, and establishing differences, commonalities, and nuances between interview data.[57]

While we understood that children undergo the changeover from childhood into adolescence at varying ages and in various ways, we designed our methodological approach by defining children as persons between the approximate ages of seven to thirteen. However, because children and adolescents are influenced by digital media environments in complicated and emerging ways, and because exposure to online extremism is of increasing interest, particularly when it involves the experiences of youths, certain questions were left unanswered within the interview timeframe and remain unaddressed. For example, in responding to the question: "to what extent are children and adolescents exposed to extreme ideological materials online?" certain interviewees concentrated their responses on components of the question (e.g. reflecting on the likelihood of exposure in specific communities) or alternative populations (e.g. reflecting on likelihood of exposure among children when compared to recent research on adult exposure) because of their former experience or current interests.[58] It is important to acknowledge that the implications of this research are preliminary, and the general trends in scholarship on child exposure to extremist content online will continue to evolve. For instance, while all policy and practice recommendations reiterated here underscore the vital role of future research and organisational policies addressing the intersection of online extremism and children's exposure, such suggestions may not have undergone critical review or undertaken developmental assessments through multi-stakeholder dialogues and multi-sectoral collaborations. Suggestions are derived from data analysis and are direct outcomes of conversations with interviewees. This limits the generalisability of this study's recommendations, as suggested by our interviewees, and invites future researchers to contextualise the findings.

## Results and Discussion

The following section presents the six overarching findings from our thematic analysis of the semi-structured interviews: (1) Vulnerability; (2) Significant Others; (3) How and Where; (4) Effects and Consequences; (5) Disciplinary Boundaries and Collaboration; and (6) Policy and Practice.

## Vulnerability

Participants highlighted the need to understand children's vulnerability to ideological imagery, symbolism, and sentiment while interacting with strangers online. Participants described the threat of misogynistic and manospheric content as a "soft entry point" into ideologically extreme communities for children. For example, the prescriptive nature of misogynistic materials among popular social media and online gaming platforms was considered attractive or striking to children – mainly male children – with anti-social propensities, interests, frustrations, insecurities, ignorance, and other social grievances characteristic of disenfranchised young men in the manosphere. Experts forecasted that misogynistic content common to manospheric movements online would become more available and more familiar through influencers on social media. For instance, interviewees had speculated that an incremental introduction to themes and personalities within the manosphere would evoke "positive associations" between "six-year-old" children and influencers such as "Andrew Tate". As one interviewee described:

> *And she [teacher] kind of had to make sure (...) that they kind of have an understanding of who this person is [Andrew Tate] because you can imagine other people, you know, Googling what is this name? Wanting to learn about it, or even if just the encounter later, they already have the familiarity. And so, familiarity can breed the trust. (...) it's kind of like sowing the seeds of harm among like a six-year-old kid, which I found pretty shocking." (...) "even just like hearing the name Andrew Tate early on as part of a (...) meme that you found enjoyable, you know, there's a positive association there.*

Experts suggested that children are also especially susceptible to adopting the ideological qualities of online materials they are exposed to, including characteristics and demeanour of the personalities. Whether this be misogynistic materials or a significant cultural figure like Andrew Tate, experts described the danger of extreme ideologies when partnered with additional markers of authority, such as the number of "followers" or its presence on popular social media or online gaming platforms readily available to children.

Other respondents focused on the psychological appeal – the desirability, suitability, and attractiveness – of extremist materials. Simplistic thought processes represented in such materials were considered potentially persuasive to children at their stage of psychological development, including the way materials construct a persistent enemy or embolden hyper-reductionist obsessions with something or someone. For example, extremist ideologies or communities that appeal to children's lifestyles using popular subcultural symbols printed on clothing or referenced in music to facilitate the child's identification with ideological assumptions therein. Interviewees highlighted the persuasiveness of these strategies because of children's sensitivity and underdeveloped capacity to negotiate their social status, reaching out to external – material or virtual – representations of social value to "fit in with their peers". As several interviewees noted, implicit in this is the tendency for ideological materials to incrementally enter digital media environments. Rather than being rapidly inundated with this material, this titrated exposure works to gradually increase the normalisation of hatred and decrease children's "moral resilience" over time. As one interviewee described:

> *the nature of exposure is largely like second-hand smoke. You know, you're exposed in so many ways to everyday racism and every day, you know, structural sexism, structural racism, the structural discriminations of so many kinds that their exposure to actual violent extremist ideological content might be lower. But this sort of everyday exposure to these types of discriminations at a less extreme level...I would suggest it probably lowers their resilience to what could then lead down the road towards a violent extremist ideological content.*

Mainstreaming extremism in this way, children and adolescents were referred to as "intermediaries" between common political content and more extreme ideological communities.

Combining familiar features from children's much-loved social media platforms or online gaming communities with controversial conversations or inflammatory content was hypothesised to increase children's vulnerability to online extremism and recruitment. Interviewees noted that this combination of platform design, taboo extremist ideas, and the capacity to interact with these features anonymously and without supervision was described as an overstimulating environment that significantly heightened the risk of ideological indoctrination. One respondent referred to this environment as "identity fusion" among children who develop a visceral impression of belonging to the online gaming community, behaving in unprecedented ways socially and culturally to obtain and maintain social status, and to address emergent psychological and physiological challenges during the child's transition into adolescence. Research supports this, indicating that identity fusion, particularly in gaming spaces such as *Call of Duty*, is strongly associated with antisocial outcomes like aggression, sexism, and racism, especially among lonely or insecurely attached individuals.[59] Another participant identified the design of online gaming architecture as fundamental to  building  trust between children and online strangers, such as when playing together on a "mission… to kill the dragon". Subsequently, respondents clearly differentiated that, while online extremism is not synonymous with radicalisation to violence, the results highlight the importance of the sociotechnical context to understand whether these digital media environments are facilitating cognitive openings or facilitating maladaptive behaviours.

Other participants described intrinsic cognitive-psychological traits that influence children's interaction with online extremist content, including curiosity. For example, one participant provided a rather constructive and counterintuitive observation about the potentially positive (albeit accidental) consequence of being exposed at an earlier age. During this participants' own professional research of young adults and online extremism, the young adults described that their curiosity somewhat insulated them from its harm and, instead, fashioned motivation to better comprehend its character through higher education. Subsequently, this finding signifies the probability that some experience in childhood development can reassure a child that their exposure to such content is not entirely or irredeemably harmful, but another object or reason to be inquisitive without becoming radicalised.

Some interviewees indicated that children who face certain adversities and traumatic experiences may be particularly sensitive to invitations – whether well-intentioned or malevolent – to be a part of a community offering social belonging. One expert suggested that children who experience offline challenges and lack digital literacy are more likely to pursue online connectivity. Another respondent suggested that teachers and parents who are ignorant of the possible harms of online extremism, as well as an absence of protective measures in the child's social media or online gaming platforms, can also increase their vulnerability. Among other participants, a significant risk factor revolved around the lack of digital media and gaming media literacy among teachers, parents, and the child's local community. As one participant suggested, "I think the biggest risk factor is the lack of gaming media literacy in parents and teachers." Another respondent noted that children are more predisposed to be introduced and exposed to online extremism if their parents are participating in such communities. This highlights the importance of digital media safety and literacy within and across familial, community, and educational settings.

Promoting community engagement and parental discussions about child safety online is subsequently critical. For instance, recent scholarship has suggested a "two-step decision tool" for monitoring children's technology use.[60] In the first step, parents monitor their children's reactions to games, websites, and apps, watching for signs that their attention is being "co-opted", "out of control", and "not self-directed", as it otherwise would when engaging in activities such as building blocks, painting, or storytelling. The second step recommends that online activities be community-supported. This involves a parent or community member discussing the child's online activity with them, allowing the child to demonstrate their ability to share and explain their reasoning while online. Ideally, this caregiver could then deliver some follow-up experiences to further reinforce learning and positive online engagement.

## Significant Others

Findings underscored the ways in which cultural figures and community members represent influential role models in children's lives. Respondents unanimously underlined the importance of "influencers" and how their parasocial relationship[61] can dramatically affect children's behaviour and worldviews.[62] Participants often referenced the recently notorious influencer Andrew Tate's captivating presence in children's digital media digests, as well as his potential to be a disruptive and hostile subject for teachers involved in classroom discussions about the influencer's "conviction" in manipulating children. Despite the combustible nature of Tate airing in classroom discussion, participants worried whether – if such topics of conversations are neglected by teachers and parents – the children's "curiosity" and "concern" may otherwise be unaddressed, leading them to further seek an audience with virtual communities who are willing to broach Tate, or other controversial online personalities. Respondents described how an influencer's contrarian dynamic may intensify the preconditions for building trust with children who – in seeking seclusion from local communities – may find opportunities to connect with them. For example, children may suppose the influencer has authentically appealed to their curiosity and expressed their concerns more than people in the children's community or daily lives. This parasocial relationship allows influencers like Tate to display themselves as "trusted sources of expertise" and offer "explanations" for grievances unbeknown to the child prior to being exposed to their content. When influencers present authority, authenticity, and charisma, the respondents suggested that children may no longer feel entirely comfortable freely expressing their influencers' opinions publicly, if their parents and community figures do not understand or agree, developing their parasocial relationships in isolation.

When providing a formulated lifestyle and social philosophy to children sympathetic to authority and certainty, almost all interviewees recognised the naivety of children who are exploited in influencer relationships. Children may not understand that influencers may have profit-seeking intentions and something to gain from grabbing their attention and turning unbridled childhood "emotion" into more user engagement. Experts expressed their worry that this influencer phenomenon is beginning much earlier than expected in childhood. One interviewee recounted an incident where Tate's misogynistic rhetoric was expressed in the classroom among six-year-old children who directly referenced Tate's online content. Notwithstanding the fact that the children "had no idea who [Andrew Tate] was or why he was currently culturally significant", the participant described "online misogyny" as a mimetic resource for gaining social approval with disorder and playful antagonism. It is important to highlight that not all influencers intend to cause hostility in children's classrooms, but more likely, most influencers are incentivised to learn how to construct online communities with a general psychosocial appeal to attract larger audiences and, subsequently, unwittingly encircling children in their lure. What was common among interviewees was the challenge of meaningfully addressing struggles among men and boys in contemporary culture and politics, with one participant suggesting that children, too, are taking aid from digital media technologies to explore complicated subjects like: What is a man? What is masculinity? How do men and boys think and feel? How should men and boys express their thoughts and feelings? Several experts suggested there is a general scarcity of awareness and understanding among community leaders and key stakeholders in this space, raising many problems without sufficient evidence or tools to inform change.

Collaboration with teachers was considered essential to mitigating the effects of online extremism among children and adolescents. While investing in teacher training and community education was offered as an obvious stepping stone to progress, participants highlighted the lack of curricula and pedagogical initiatives that focus on children's vulnerabilities and strengths when negotiating complex political and controversial social topics. The absence of pedagogical architecture on this issue was suggested to be the consequence of a dearth of engagement with and research on teachers themselves, understanding the extent of teachers' knowledge in areas of online extremist subcultures, making educational and curriculum initiatives difficult to design. Seeing as there are few support mechanisms or much previous literature to build upon, one interviewee commented on the challenges of erecting this educational program: "You start from scratch." Instead, pedagogies, such as inquiry-based learning, open the space for students to share their reflections across the curriculum and present educators with a unique opportunity to help guide student conversations. This would then serve as a baseline from which P/CVE programs in primary or secondary schools allow spaces for the candid and controversial conversations needed to effectively address extremism.[63]

Despite these challenges, interviewees noted that the need for greater education on this topic is growing, with teachers reporting increased rates of children being targeted with extremist materials and rhetoric online. Furthermore, most experts reported their concern for the deficiency of knowledge and awareness within schools generally, highlighting instances where parent-teacher conversations sometimes degenerate into accusations of the other's inability to supervise children's online activity or comprehend the risks associated with extreme ideological content. As one interviewee stated:

> *I think especially educating teachers that the problem is not the content of the games, but the communities that form around them. Like they're still think some of them have that kind of older school model where they think about like the harms of video games in terms of like the content instead of No, it's actually like the communities that build up around them and the toxicity there. And yeah, so just getting them to understand like where, you know, where the problem is actually located could be really useful.*

A striking observation was that although none of the interviewees directly engaged parents, they acknowledged this is a significant gap in the communities' defence against extremism online. Despite parents' lack of involvement or awareness of initiatives concerning their children's protection against online extremism, most participants recognised that parents play an immense role and – in addition to teachers – also need advanced digital media skills. Interviewees hence highlighted the necessity for future research to include parent populations to understand their knowledge boundaries on online subcultures. One participant highlighted the potential of parents to unwittingly introduce racist, hateful, and extremist ideologies to their children through imitation in family contexts, which in turn emphasises the position of teachers and the school system to lead these conversations about extremism online.

## How and Where

Findings highlight the nature of sociotechnical contexts where children are exposed to extremist materials and how these contexts are changing their means of exposure. The proliferation and accessibility of digital media technologies in contemporary society have resulted in children exploring potentially threatening online communities from a younger age. Participants emphasised the diversity of digital media environments and the range of extreme ideological materials that children are believed to engage in on a routine basis, with one interviewee insisting: "Well, when it comes to children being exposed to extremist content online, I think there are a lot of different options."

For example, participants named particular social media platforms, including Facebook (or Meta), Metaverse, TikTok, and Twitter (or X), as well as specific video streaming platforms, such as YouTube and Twitch as mass news distributors, who – at times – broadcast terrorist propaganda, such as from the so-called Islamic State and the Christchurch terrorist attack in New Zealand. Additionally, online gaming platforms and adjacent communities – *Roblox, Discord, Call of Duty, Steam*, and *Minecraft* were mentioned frequently. Participants often focused on the prevalence, accessibility, and potential harms caused by mainstream gaming platforms, such as Roblox, and alternative gaming programs designed to spread hateful rhetoric and extremist sentiments. As one interviewee described:

> *It's not on the immediate surface, but pretty much as soon as you start scratching below that surface, you're going to find…it. So, while … gaming adjacent spaces are pitched as being for children and they were designed to be for younger age groups, they still harbour this type of 'people content'…So, Roblox is a good example because it's not that Roblox is putting Nazi prison guard content out there. It's that a user of Roblox is able to go into the Roblox game and build that environment themselves.*

While the design features and operative functions of online gaming platforms was concerning to participants, interviewees often concentrated on the "toxicity" of online communities that revolve around gameplay or social networks. For interviewees that are first responders, this highlighted the importance of the nature of the interconnection between children and online communities, rather than the specific subjects embedded in online materials.

This raises a question in terrorism and extremism studies more broadly: how can we distinguish between the influence of "unhealthy" or "distasteful" communities and the dynamics of intermittent messaging between peers or influencers that are considered "extremist"? Participants agreed that communities that perpetuate "low self-esteem" and "bullying dynamics" to encourage children and adolescents to engage in online extremist conversations can be dangerous and should be subject to online harm prevention measures. However, such communities or individuals therein may not necessarily be "extremist" themselves or necessitate counter-violent extremism interventions. For instance, the manospheric online space – a loosely affiliated network of digital media platforms and communities which encompass controversial political, social, and cultural issues about masculinity, men, and boys – may introduce children to various authoritative and (ostensibly) knowledgeable figures who supposedly provide "explanations" on how to overcome personal challenges thought to primarily affect men and boys. And while characteristic of certain manospheric movements are online extremist materials and communities who do perpetuate violent extremism, not every person or space in the manosphere is "extremist". For instance, interviewees suggested Jordan Peterson had established an ideological gateway toward extreme misogyny and male supremacy, but acknowledged Peterson offered – albeit "questionable" and "concerning"– advice and guidance to a much wider population of misguided young men and boys.[64, 65] This finding highlights the importance of understanding exactly how and where the level of concern transverses such communities.

For example, the concept of 'Fringe Fluidity' may be an important avenue for future researchers. Global currents of extremism materials now stream across social platforms cohabitated by communities who – once distinct – occupy overlapping areas of the virtual landscape. Users and materials at the fringe of these communities are now systematically introduced to users and materials in a corresponding fringe. Online representations of ideologies in these communities are well-documented in the field. Gartenstein-Ross and Blackman – who coined the term – identified that terrorism studies needed to better understand enabling environments and support structures that assisted "the various journeys through which people embrace violent extremism."[66] Though Gartenstein-Ross and Blackman and later Ganor suggested common denominators may provide avenues for convergence, such as revenge, glory, call to action, or emergency, many unanswered questions remain concerning how and where the convergence occurs online and especially regarding children.[67] Technological affordances offer channels of communication where children may be transported away from social networking or online gaming communities unaffected by extremist materials and toward concerning online chatrooms where extremist content is prevalent. Interviewees believed the dissemination of extremist materials through sociotechnical systems – such as "personalisation" algorithms and "share" functions – represented a "ripple" or "network effect" where exposure spreads rapidly and may unintentionally be passively presented to children in an adjoining online community. Interviewees identified "network features" that likely contribute to this phenomenon, such as "voice chat" and "text-based chat communication" during a "team-based" interaction with strangers in "open online games." Some respondents suggested consulting specific individual communities to moderate their own cultural space. This was suggested to be customary for administrators on Reddit to moderate conduct and encourage their communities to self-regulate. Alternatively, other experts emphasised the necessity for researchers to initiate conversations with people responsible for designing and implementing such protective measures at social media companies and online gaming companies, so as to share knowledge and technical expertise to mitigate the likelihood that young viewers are affected by online extremism existing underneath the terms of service thresholds currently in place or overwhelming content moderation efforts.

## Effects and Consequences

Findings indicated the dearth of evidence regarding psychological or physiological consequences of early childhood exposure to extremist materials. Two participants provided anecdotal evidence of two incidents having involved children who expressed thoughts or feelings related to extremist ideologies following their presumed exposure. One incident involved a child making an anti-government comment during a classroom discussion (i.e. "calling for the death of the Prime Minister"). In the other example, a male child was alleged to have been "punched in the face" by a female child, but the student's motivation was unknown. Nevertheless, almost all interviewees suggested there were significant potential social and psychological effects from exposure and claimed incidents of hate-motivated rhetoric and behaviours were becoming more frequent (though no other incidents were presented or discussed). When asked, participants struggled to identify psychological conditions thought to manifest after exposure, suggesting that based on cyberbullying literature, children have the potential to develop "anxiety or depressive disorders" from observing ideologically extreme and hate-related extremist content online. Regarding sociological effects, some respondents suggested that the specific outcomes would likely correspond with the type of ideological materials being viewed online. For example, interviewees speculated "siege culture"[68] may embolden children's interest in extremist ideologies, or "manospheric culture" may encourage children to normalise homophobic narratives.[69] Seeing as almost all respondents indicated they were unaware or unable to specify the psychological or physiological effects of exposure, addressing this knowledge gap requires a nuanced understanding of the underlying propensities and motivations of children's cognitive-psychological dynamics, in addition to the character of the ideological content observed. Drawing on existing research on the psychological effects of violent media exposure in adolescents and adults offers an empirical foundation for understanding the impact of exposure to extremist materials in the future.[70] Building on these insights, future research should focus on how exposure to extreme forms of media specifically affects younger children, accounting for their unique developmental needs and capacities.

Furthermore, several study participants described how risk is manifest in the way children move from engaging in an online game or with social media materials to interacting with the wider social community or group around it, stressing that susceptibility towards online harms lies in certain interactions that can be manifested within social online communities and semi-public spaces. Although empirical research on this acute dynamic is by and large absent, critical observations are beginning to evolve in the form of case studies, systematic reviews, and discussions.[71] For example, although not focused on children, Hassan and colleagues repeatedly found that exposure to radical violent online material can encourage or advance violent extremist acts, opinions, and motivations among younger demographics.[72]

## Disciplinary Boundaries and Collaboration

Findings strongly highlighted the methodological and institutional barriers to research. Interviewees identified several pragmatic problems pertaining to timing research with schooling systems and teacher timetables, such as collecting data in school semesters, in addition to difficulties in finding channels of communication when recruiting study participants, particularly parents where such contact was considered "unreliable". Ethical sensitivities when studying vulnerable populations, such as children, political sensitivities when conducting research on "violent extremism" in schools with public reputations, and the consequences of the pandemic lockdowns, among other legal requirements, significantly constrained access to children or blocked scientific research entirely. Engaging with parents was generally considered difficult, particularly among seemingly apathetic parents who "don't care" about online safety or online harm. One participant stated their unwillingness to engage: "the parent-child relationship is something that we don't really get into too much because it is too contentious." This is problematic as participants and the literature suggest the importance of offline experiences in contributing to children's vulnerability to online extremist content. However, due to limited access to lifestyles, the participants were generally unsure of what was "missing" from children's lives to feel compelled to engage in extremist conversations. Regardless of the possible effects, findings highlight the difficulties that prevent researchers and policy-makers from probing children's exposure to online extremism, resulting in – as one participant stated – "the nature of exposure is therefore unknown."

Aside from accessibility to school communities, interviewees noted the difficulty in documenting "intentionality" in online extremist communities that are allegedly narrowcasting to children for indoctrination and recruitment purposes. Respondents suggested the ambiguity of "groomer offline identities" is - due to both age and identity verification on social networking and online gaming platforms - being largely absent. This represents a major obstacle to understanding "whether extremist groups are actually strategically talking to children or whether it is more opportunistic." This suggests that scholars primarily use indirect measurements of "intentionality" on a case-by-case basis. As a result, the interviewees in this research wondered whether and to what degree components of these digital media environments facilitate childhood exposure, such as what degree is target vs organic recruitment facilitated by gaming infrastructures and unintentional exposure due to social media algorithmic selection applications. In addition, and depending on the measurements taken, expert assessments concerning the seriousness and danger of exposure can be significantly different, as some noted that the problem of online recruitment of children is considerable and should be of more concern to others, while their colleagues suggested recruitment among children "is relatively low" and not the "main concern with gaming networks."

Evident in almost every interview was the boundary between disciplinary domains like terrorism studies, media and communication studies, education, child developmental psychology, and cognitive-psychological sciences. Almost all interviewees overwhelmingly highlighted the scant interdisciplinary collaboration with cognitive-psychology sciences in general and child developmental psychologists in particular. While almost every participant voiced their intuitions about the cognitive-psychological consequences or assumed developmental trajectory of children and adolescents, experts often punctuated their speculation with a comment acknowledging the limit of their disciplinary knowledge was reached, including: "But, I'm not a child psychology expert, so I'm not qualified really to answer that question."

The dearth of cognitive-psychological science and child psychological expertise has consequences for how participants conceptualised the importance and influence of developmental stages in correspondence with children's vulnerability or the effects of exposure to online extremism. Regardless, qualities or processes pertaining to child neurological and psychological development were considered to be foundational to understanding their vulnerability to online extremism, such as "distorted cognition" and "deficits in abstraction", "rational thinking", "maturity", "empathy", "prudence", or capacity to regulate status seeking or risky behaviour during socially and psychologically exploratory phrases of their life. One participant noted, for example, that children's identity and validation are of primary importance, meaning that their neurological plasticity and degree of impressionability are at their assumed maximum (referred to as "sponge"-like), which leaves them considerably more vulnerable to the absorption of online extremist content. Furthermore, children's development and assumed sensitivities were employed liberally in hypothetical accounts of the "online radicalisation process" or "pathways" available to children. This includes the "obvious" significance of cognition in creating justifications for indoctrination or violence among children, such as children's incapacity to "think critically" or "abstractly" defines their "decision-making process" when exposed to ideologically extreme materials, or "neurodivergent" children especially vulnerable to online recruitment. For example, interviewees suggested that an "autistic child" may experience online gaming communities as an emotionally unintrusive environment, and such positive social parameters increase their susceptibility to grooming strategies. These findings suggest future research and policy initiatives ought to involve more interdisciplinary contributions in a spirit of consilience, spanning natural and social sciences.

Such collaborations are thought to close the distance between researchers and children's understanding of what "extremist" actually means. One participant highlighted the broad disparity between what researchers think extremism, in fact, ought to be and what children believe extremism materials are. For example, when discussing extremist online materials with young adult participants in a previous study, one interviewee found their participants considered imagery depicting animal brutality in nature as well as sexual violence to be "extremist material". These findings highlight the importance of placing aside terrorism frameworks to become more acutely aware of what children and youth perceive online extremism to be in the first place. As one interviewee highlighted:

> *"as a terrorism academic, you can sometimes get caught up in your own area and think it is more important than it actually is", and because of this, "we often don't see the stuff that [young people] are finding extremist and even violent extremist."*

## Policy and Practice

Findings highlight the importance of complex and multifaceted interventions across various systems. Some interviewees described skill-based education that involves instructing school-aged students in digital media verification practices to ascertain whether the information they perceive online is likely to be true or false, then discussing the effects of their judgments with teachers, for example. However, such interventions have been considered insufficient or even misleading, when used narrowly to decrease children's vulnerability to online extremism. For instance, one respondent believed that recent proliferation of misinformation and disinformation campaigns had convoluted the meaning or purpose of the in-classroom verification practices in the context of countering extremism on children. Furthermore, teaching verification practices become more advanced when coupled with contextualisation practices designed to teach children how to think about their place in the digital media landscape when assessing individual bits of online content. As one participant proposed, children should be equipped with a level of "healthy scepticism" about online materials.

Other participants suggested that children begin by improving their understanding of themselves and their involvement in digital media environments, recommending that children regularly self-reflect on and monitor their digital media consumption habits. These "mindfulness" practices – as some interviewees believed – developed a more mature sense of self-awareness and self-regulation in consuming or confronting online extremist content. This includes pedagogies to assist children in understanding how online games and surrounding communities can be "highly emotional places" – "competitive", "combative", "arousing", "hyper-stimulating" – where their psychological safety, identity, and opinions can be significantly affected. Participants understood self-regulatory practices to support children's resistance against all manner of pathologies related to online extremist content, with one participant suggesting cognitive behavioural techniques holding a greater presence in interventions preventing online harm.

At the community level, one participant suggested a larger initiative to build trust between children and their local community as a primary prevention measure, while another suggested introducing community-oriented civic education or civic intentionality into classroom discussions and curricula. Various participants suggested multi-level or cross-sectoral approaches in order to bring together an audience of diverse stakeholders to engage in constructive dialogues, raise awareness of technical solutions and social initiatives, and specifically decrease the likelihood of harm caused by online extremism. One participant recommended bringing together academia and law enforcement (e.g. "digital police officers") to collaboratively engage this phenomenon. Several highlighted the value of design interventions during the production of gaming software, where software developers can implement designs that are resistant to extremist exploitation into their online gaming platforms. Design-oriented approaches to large-scale technological innovations were considered an important industry, ideal to encourage  multi-stakeholder meetings; with online gaming, augmented reality, and virtual reality gaming platforms in continuous development, safety-by-design approaches are likely to become an effective strategy for avoiding future online harms.

Additionally, several participants remarked that online gaming companies ought to be increasingly aware of the implications of their platforms when cultural narratives are manipulated for online extremist ends (e.g. ancient Nordic cultures and religions in the games

"God of War: Ragnarök" and "Assassin's Creed: Valhalla"). Participants also suggested mandatory regulation and indexation to mitigate online harms around products used by children, such as age verification filters on Roblox and Minecraft, for instance. However, none of the interviewees advised on the exact measures or technical mechanisms required to ensure security across the various demographics playing in – for example – online gaming communities. In answer to this, respondents often encouraged greater collaboration with software developers, social media companies, and online gaming companies. As one participant stated: "Why aren't we there? We are political scientists, criminologists, and social workers. We're not game developers; that's an area we should look at, too."

However, the historical stigmatisation of online gaming cultures makes the potential for collaboration difficult, especially when "interventions" are raised for young gamers. Respondents cautioned about the nature of anti-gaming stigma in building relationships between those who study online extremism and those who are potentially exposed to online extremism in online gaming communities. One respondent was particularly vocal about exacerbating children's perceptions and opinions of their community as untrustworthy, irrelevant, and contradictory to the community's interests or country's values. Pathologising children's good-natured "past-times" (i.e. video games) as a "pathway to online radicalisation" and a threat to national security may create barriers to social and cultural progress, particularly because these interests are not necessarily harmful in and of themselves. Additionally, by prioritising community-orientated and institutional approaches, we effectively reposition the responsibility from individuals (e.g. parents, teachers, and children) to "prevent" or "solve" online extremism, and redistribute this burden to broader structural institutions of the Internet and wider societal institutions. Regarding the latter, for some interviewees, this meant collaborating with community-based organisations and secondary socialisation agents, such as kindergartens, early childhood education, schools, social workers, and libraries. These considerations are reflective of systematic reviews of P/CVE measures and interventions that were recently evaluated internationally.[73]

Accordingly, this study's policy recommendations – that emerged from the results of our data analysis – highlight the importance of future policies and practices when developed during multi-stakeholder discussions and multi-sectoral approaches, including:

- Develop and make available pre-service preparation and in-service training programs in digital media pedagogies and provide access to relevant information technology resources within schools for educators and administrators targeting early childhood, primary, and secondary school settings to raise awareness on online subcultures and enhance digital media literacy.

- Expand the integration of comprehensive digital media literacy into early childhood and school policies, curricula, and continuing education initiatives.

- Establish school-based awareness and support programs to foster open and authentic dialogues among parents and caregivers regarding online contexts and the safety of children's online activities.

- Enhance the capacity of local community-based organisations to develop educational campaigns and materials, focusing on empowering parents to guide their children in navigating social media and engaging in digital communities, including gaming culture and online misogyny within these spheres.

- Improve and assess the efficacy of platform design elements such as age verification measures, algorithm transparency, robust data protection policies, age-appropriate features, and content moderation practices by social media and online gaming companies. This should include greater effort to tailor terms of service agreements and community guidelines to meet the needs of young children.

- Engage front-line practitioners, such as social workers and mental health professionals, in initiatives supporting educators and parents in managing children's online and offline wellbeing and mental health.

- Create platforms for parents and children to share their experiences with online gaming and social media with community researchers, fostering future research initiatives and advocacy with policymakers for social change.

## Limitations

There are a few limitations associated with this study. Readers should be cautious in generalising the findings or recommendations presented in this study to their respective contexts and areas of practice. Although interviewees note the variety of risks and the protective factors concerning child exposure to extremist online content and underscore the multifaceted interventions needed to tackle the issue, the findings and recommendations proposed ought to be further contextualised and applied in future intersectoral research. Additionally, the relevance of the recommendations in policy and (or) practice will be disproportionate to the context in which they are applied and we cannot anticipate how contextual factors will alter the applicability of one or another recommendation. The recommendations presented have considerable empirical overlaps between theoretical literature and the professional experiences as referenced by these interviewees. This investigation only interviewed adult experts who provided insights and professional experiences regarding youth and children's exposure to extremism online. This study did not interview children or adolescents.

## Conclusion and Outlook

This article offers a preliminary expert assessment of the effects of early childhood exposure to online extremist materials. In reviewing key literature and conducting expert interviews, our research reveals critical dimensions of the issue and normative aspects of online extremism, stressing the psychological appeal and potential of extremist content to dually appeal to children and adolescents organically including through algorithmic technology, as well as exacerbate the frustrations in disenfranchised children and adolescents.

In bringing together the recommendations from the international experts who participated in this study, there are a number of main themes to help guide research, programs, and policymakers to better understand and address this still nascent area of concern. Overall, these recommendations suggest a multifaceted approach, prioritising awareness and nuanced digital media literacy training in schools and the wider community. Parental and teacher involvement is a fundamental theme in what experts discussed, which could include monitoring of children's online activities, empowering children with critical competencies for informed risk-taking, digital media use, and participation in networks of digital media environments. Greater practitioner involvement – in particular social workers and child developmental psychologists – was also a strong, common call among experts for supporting teachers and parents in this endeavour. They also encourage local communities to collaborate in education programs and safety workshops. Importantly, they also suggest that technology companies further invest in safety-by-design approaches, including  considering age and identity verification measures to enhance content moderation and security measures, in addition to producing terms of service conditions and community standards for populations of children users. Study participants also emphasised that managing children's online activities and mental health concerning online extremism should encompass more scholars and practitioners alike outside of terrorism and countering violent extremism studies. They urge more interdisciplinary research for a comprehensive understanding of the effects of early childhood exposure and the creation of effective prevention strategies.

While all interviewees pointed toward the role of school-based education, scholarship continues to identify several structural barriers that lie within the school system that make integrating P/CVE measures an enduring challenge to researchers and practitioners. With regard to classroom discourse in general, earlier research has found that teachers have difficulty structuring it and oftentimes do not offer dialogic bids to their students, resulting in limited capacity to have authentic dialogue around controversial issues.[74] Structural barriers also include the overlooked issue that schools are 'by-in-large' undemocratic spaces and the impact on marginalised communities as contributing factors to children's vulnerability to extremist content. Firstly, in various countries, undemocratic schools often fail to cultivate environments that support critical thinking and active student participation in democratic processes. These schools might not prioritise teaching methodologies that encourage questioning, independent thought as well as life and career skills, making students more susceptible to accepting extremist narratives without critique.[75] Secondly, the impact on marginalised communities and emerging economies remains a significant concern. In developing countries, equal access to education remains a challenge, and a lack of safe spaces in these schools means that students are unable to effectively practice the critical thinking skills needed to build resilience against the allure of radicalisation.[76] This also has profound impacts on teachers; research suggested to take into account the contextual description of violence teachers have experienced and to develop trauma-informed pedagogies for teacher education.[77] Related challenges include teacher burnout and shortages, as well as access to social support systems for front-line professionals.[78] In countries such as the United States, both rural white students and racial and ethnic minorities are often relegated to underfunded and under-resourced schools.[79] These disparities in educational resources and quality may exacerbate the vulnerability of children in these communities to online extremist content. Schools in marginalised communities often lack the necessary support to address the unique challenges faced by their students, which can contribute to individual susceptibility and undermine social cohesion. Promoting equitable access to quality education, along with robust support systems and the fostering of critical thinking and citizenship education, is crucial for empowering students to challenge extremist ideologies and engage actively in democratic processes.[80] Digital tools, such as child-friendly websites and large language model-based artificial intelligence, offer an opportunity to revolutionise primary and secondary education, making education and learning more student-centred and engaging. These tools support personalised, inquiry-based, and collaborative learning approaches, allowing students to generate their own questions and seek answers through self-directed research and problem-solving.[81] This approach also enhances critical thinking, a skill that needs to be integrated throughout the curriculum and community initiatives to counteract extremist narratives effectively.

Ultimately, this study emphasises the importance of greater collaboration with multi-stakeholder communities, moving beyond teacher-centric or technology-centric solutions. Additionally, contemporary barriers to child-centred research and policy development need to be reconsidered to advance knowledge in primary and secondary education, focusing on community support networks, democratic education, teacher and student support, and sustainable technology practices. This perspective – as shared by most of the interviewees – supports the preventative design approach and collaborative policies based on future empirical insights on parent-child behaviour and understanding of best practices for decision-making in this digital age. These expert assessments were intended to lay a foundation for future research and policy initiatives, emphasising the need for safety-, collaboration-, and well-being-focused conversations among stakeholders to share knowledge in developing solutions.

*Jade Hutchinson (Cotutelle PhD, MPhil, B.I.S) is a Post-Doctoral Fellow within the Faculty of Social Sciences' Department of Security Studies at Charles University (Czech Republic). This work was supported by the Cooperatio program, research area Political Science. ORCHID ID: 0009-0001-4510-3375, jade.hutchinson@mq.edu.au*
*LinkedIn: https://www.linkedin.com/in/jade-hutchinson-981984bb/*

*David Yuzva Clement (Ph.D., M.S.W., M.A.) is an Adjunct Research Professor in the School of Social Work at Carleton University (Canada), Associate Fellow at the International Centre for Counter-Terrorism (Netherlands), co-Founder of the Inter-Faith Peace Initiative Bonn (Germany), and Research Advisor at the Canada Centre for Community Engagement and Prevention of Violence (Canada). https://orcid.org/0009-0001-0835-3711*

*Ruxandra M. Gheorghe (M.A., M.S.W., R.S.W.) is a doctoral candidate at Carleton University's School of Social Work in Ottawa, Canada. Alongside her research, Ruxandra is also a Lecturer in Carleton University's School of Social Work, a Registered Social Worker practicing in clinical mental health, a Senior Fellow at the Canadian Institute for Far-Right Studies, and a Research Advisor at the Canada Centre for Community Engagement and Prevention of Violence.*
*https://orcid.org/0000-0002-7523-4376*

*Lorraine Kellum was trained at Virginia Tech, where she earned an M.A. in Education and a B.S. in Psychology/French Language and Literature, specializing in democratic and globally-minded educational practices. Currently based in Brussels as an Enterprise Specialist at Teachstone, Lorraine supports educational initiatives across Belgium, the Netherlands, Italy, and Japan, including the role of education in building resilience against radicalization and the influence of cultural diversity in P/CVE. lorrainejkellum@hotmail.com*
*https://orcid.org/0009-0008-7978-3744*

*Alexander Shuttleworth is a psychology student in the School of Psychology at the University of New South Wales (Australia) and an New South Wales Government Registered Nurse. Alex's research involves using animal models to explore how social experiences influence the ability to utilise social support systems effectively during trauma coping processes, with potential implications for therapeutic interventions and policy development. alex.j.shuttleworth@gmail.com*

# Endnotes

1 Joe Pinkstone, "Kids Spend Twice as Long on Their Phones than Talking to PARENTS," *Mail Online*, February 8, 2019, https://www.dailymail.co.uk/sciencetech/article-6682103/Kids-spend-twice-long-smartphones-talking-PARENTS.html; Global Myopia Awareness Coalition, "US Children/Teens Who Have Spent More than Four Hours Daily Using Electronics Devices Before vs. During the Coronavirus Pandemic, by Age, June 2020 (% of Respondents in Each Group)," *Insider Intelligence*, 8 July , 2020, https://www.emarketer.com/chart/240284/us-childrenteens-who-have-spent-more-than-four-hours-daily-using-electronics-devices-before-vs-during-coronavirus-pandemic-by-age-june-2020-of-respondents-each-group. Chassiakos, Yolanda (Linda), Jenny Radesky, Dimitri Christakis, Megan A. Moreno, Corinn Cross, COUNCIL ON COMMUNICATIONS AND MEDIA, David Hill, et al., "Children and Adolescents and Digital Media." *Pediatrics* 138, no 5 (2016): e20162593, https://doi.org/10.1542/peds.2016-2593; Lazonder, Ard W., Amber Walraven, Hannie Gijlers, and Noortje Janssen, "Longitudinal Assessment of Digital Literacy in Children: Findings from a Large Dutch Single-School Study," *Computers & Education* 143 (January): 103681 (2020), https://doi.org/10.1016/j.compedu.2019.103681; MPFS, "JIM-Studie 2022: Basisuntersuchung Zum Medienumgang 12- Bis 19-Jähriger," Germany: Medienpädagogischer Forschungsverbund Südwest, 2022, https://www.mpfs.de/studien/jim-studie/2022/.

2 Chassiakos, Yolanda (Linda), Jenny Radesky, Dimitri Christakis, Megan A. Moreno, Corinn Cross, COUNCIL ON COMMUNICATIONS AND MEDIA, David Hill, et al., "Children and Adolescents and Digital Media." *Pediatrics* 138, no.5 (2016): e20162593, https://doi.org/10.1542/peds.2016-2593; Schurgin, Gwenn Schurgin, Kathleen Clarke-Pearson, and Council on Communications and Media, "The Impact of Social Media on Children, Adolescents, and Families," *Pediatrics* 127, no. 4 (2011): 800–804, https://doi.org/10.1542/peds.2011-0054.

3 Colliver, Stacey, James Popham, Samantha Henderson, Sarah Daly, and Lucas Pokrywa, *Tracing Radicalisation to the Incel Movement and Its Connection to Loneliness,* Knowledge Synthesis Grant Final Report (Canada, 2022), https://researchcentres.wlu.ca/centre-for-research-on-security-practices/assets/documents/incel-ks-report.pdf.

4 Caton, Sue, and Roderick Landman, "Internet Safety, Online Radicalisation and Young People with Learning Disabilities," *British Journal of Learning Disabilities* 50, no. 1 (2022): 88–97. https://doi.org/10.1111/bld.12372; Koehler, Daniel, Verena Fiebig, and Irina Jugl, "From Gaming to Hating: Extreme-Right Ideological Indoctrination and Mobilization for Violence of Children on Online Gaming Platforms," *Political Psychology* 44, no. 2 (2023): 419–34, https://doi.org/10.1111/pops.12855.

5 Eccles, J. S., "The Development of Children Ages 6 to 14", *The Future of Children* 9, no. 2 (1999): 30–44.

6 In this article, mimicry refers to the act of imitating or replicating behaviours, attitudes, or expressions observed in a social or digital environment. In the case of online misogyny among children, mimicry involves replicating the harmful behaviours and attitudes towards women that are prevalent in digital media environments. This type of reactive engagement may manifest in sharing, liking, or creating content that objectifies, demeans, or devalues women, thereby perpetuating harmful stereotypes and behaviours. The act of mimicry in this context is not just a passive observation but an active participation in the perpetuation of harmful norms and attitudes, often without fully understanding the implications or consequences of such actions.

7 Andrew Tate is an American-British media personality, businessman, and former professional kickboxer. He gained wider attention in 2016 when he appeared on the British TV show Big Brother but was removed after a video appeared to show him attacking a woman. Tate gained more widespread recognition through his presence on social media platforms like Twitter (X) and YouTube, where he often shares his views on various topics, including relationships, masculinity, and 'self-improvement'. However, his opinions and statements are highly controversial and have attracted criticism for being misogynistic, offensive, violent, and insensitive. Tate has been involved in various controversies, including making inflammatory remarks on social media and being banned from platforms like Twitter (X). For instance, Tate has been charged in Romania with rape, human trafficking, and forming an organised crime group to sexually exploit women, as well as making inflammatory remarks on social media and subsequently becoming deplatformed on multiple platforms for violating their terms and policies. Tate has been described as a "self-help guru" and accused of running a "cult of control", offering his (mostly male) virtual communities highly controversial guidance and advice, such as "recipes for making money", "pulling girls", and "escaping the matrix."

8 BBC News, "Who Is Andrew Tate? The Self-Proclaimed Misogynist Influencer," 30 December, 2022, https://www.bbc.com/news/uk-64125045; Shanti Das, "Inside the Violent, Misogynistic World of TikTok's New Star, Andrew Tate," *The Observer*, 6 August, 2022, sec. Technology, https://www.theguardian.com/technology/2022/aug/06/andrew-tate-violent-misogynistic-world-of-tiktok-new-star; Angela Nagle, "The Lost Boys,"*The Atlantic*, 14 November, 2017. https://www.theatlantic.com/magazine/archive/2017/12/brotherhood-of-losers/544158/; Brittany Shammas, "TikTok and Meta Ban Self-Described Misogynist Andrew Tate," *Washington Post*, 22 August, 2022,

https://www.washingtonpost.com/technology/2022/08/21/andrew-tate-tiktok-instagram/; Lucy Williamson and George Wright, "Andrew Tate Charged with Rape and Human Trafficking," 20 June, 2023, https://www.bbc.com/news/world-europe-65959097.

9 Albert Bandura, "Social Cognitive Theory of Mass Communication," *Media Psychology* 3, no. 3 (2001): 265–299, https://doi.org/10.1207/S1532785XMEP0303_03.

10 We acknowledge the complexity and overlapping meanings of terminologies relevant to early childhood exposure to online violent extremism. While the scope our study necessitates a certain level of generalisation, we have included descriptive definitions to guide the reader and contextualise our findings. For example, in brief, by "extremist propaganda", we refer to media content explicitly designed to promote extremist ideologies and recruit followers, which may include videos of terrorist attacks. "Extremist material" is a broader term that includes any content promoting extremist views, such as manifestos and speeches. "Online hate" refers to digital content that spreads hatred against specific groups, which may include insults and devaluation of these groups. "Violent extremism online" encompasses content that incites or glorifies violence for ideological reasons.

11 Randy Borum, "Radicalization into Violent Extremism I: A Review of Social Science Theories," *Journal of Strategic Security* 4, no. 4 (2011), http://dx.doi.org/10.5038/1944-0472.4.4.1; Maura Conway,"Determining the Role of the Internet in Right-Wing Extremism and Terrorism: Nine Suggestions for Progressing Research," Presentation, The Avert Network: Online Series, December 9, 2020; Daniel Koehler, "The Radical Online: Individual Radicalization Processes and the Role of the Internet," *Journal for Deradicalization* , no. 1 (2014): 116–34; Ryan Scrivens, "Exploring Radical Right-Wing Posting Behaviors Online," *Deviant Behavior* (2020): 1–15, https://doi.org/10.1080/01639625.2020.1756391; Alex Schmid, "Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review," *Terrorism and Counter-Terrorism Studies* (2013), https://doi.org/10.19165/2013.1.02; Winter, Charlie, Peter Neumann, Alexander Meleagrou-Hitchens, Magnus Ranstorp, Lorenzo Vidino, and Johanna Fürst, "Online Extremism: Research Trends in Internet Activism, Radicalization, and Counter-Strategies," *International Journal of Conflict and Violence (IJCV)* 14 (2020):1–20, https://doi.org/10.4119/ijcv-3809.

12 Radicalisation Awareness Network, "Integrating the Online Dimension into Offline Pedagogical Practices," RAN Conclusion Paper, European Commission, 2022, https://home-affairs.ec.europa.eu/system/files/2022-06/ran_y-e_integrating_online_dimension_into_offline_pedagogical_practices_8-9032022_en.pdf; Behr, Ines von, Anais Reding, Charlie Edwards, and Luke Gribbon, "Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism," RAND Corporation, 2013, https://www.rand.org/pubs/research_reports/RR453.html; Daniel Koehler, "Violent Extremism, Mental Health and Substance Abuse among Adolescents: Towards a Trauma Psychological Perspective on Violent Radicalization and Deradicalization," *The Journal of Forensic Psychiatry & Psychology* 31, no. 3 (2020): 455–72, https://doi.org/10.1080/14789949.2020.1758752.

13 Michael Wolfowicz, Badi Hasisi, and David Weisburd, "What Are the Effects of Different Elements of Media on Radicalization Outcomes? A Systematic Review," *Campbell Systematic Reviews* 18, no. 2 (2022): e1244, https://doi.org/10.1002/cl2.1244; Özen Odag, Anne Leiser, and Klaus Boehnke, "Reviewing the Role of the Internet in Radicalization Processes," *Journal for Deradicalization*, no. 21 ( 2019), 261–300; International Centre for the Study of Radicalisation, "ICSR / VOX-Pol Paper – Research Perspectives on Online Radicalisation: A Literature Review 2006-2016," *ICSR* (blog), 3 May, 2017. https://icsr.info/2017/05/03/icsr-vox-pol-paper-research-perspectives-online-radicalisation-literature-review-2006-2016-2/.

14 It is important to note that organic gaming is not exclusive to situations where online extremist content is involved. It also refers to the strategy of attracting gaming players through unguided social processes, including the word-of-mouth, positive reviews in gaming publications, and social media activity. While organic gaming can be effective in generating initial interest, it is not the most reliable or scalable method for sustaining or growing interest in one or another gaming platform or community.

15 Patty Toledo, "Building a Community vs. Organic Player Acquisition in Gaming," Creative Raids: LinkedIn., 2023, https://www.linkedin.com/pulse/building-community-vs-organic-player-acquisition-gaming-patty-toledo/

16 Aoife Gallagher, Ciarán O'Connor, Pierre Vaux, Elise Thomas, and Jacob Davey, *Gaming and Extremism: The Extreme Right on Discord*, Institute for Strategic Dialogue (2021), https://www.isdglobal.org/isd-publications/gaming-and-extremism-the-extreme-right-on-discord/; Daniel Koehler, Verena Fiebig, and Irina Jugl, "From Gaming to Hating: Extreme-Right Ideological Indoctrination and Mobilization for Violence of Children on Online Gaming Platforms," *Political Psychology* 44, no. 2 (2023): 419–34, https://doi.org/10.1111/pops.12855.

17 Aoife Gallagher, Ciarán O'Connor, Pierre Vaux, Elise Thomas, and Jacob Davey, *Gaming and Extremism: The Extreme Right on Discord*, Institute for Strategic Dialogue (2021),

https://www.isdglobal.org/isd-publications/gaming-and-extremism-the-extreme-right-on-discord/; Daniel Koehler, Verena Fiebig, and Irina Jugl, "From Gaming to Hating: Extreme-Right Ideological Indoctrination and Mobilization for Violence of Children on Online Gaming Platforms," *Political Psychology* 44, no. 2 (2023): 419–34, https://doi.org/10.1111/pops.12855; Menso Hartgers and Eviane Leidig, "Fighting Extremism in Gaming Platforms: A Set of Design Principles to Develop Comprehensive P/CVE Strategies," International Centre for Counter-Terrorism – ICCT, June 1, 2023. https://www.icct.nl/publication/fighting-extremism-gaming-platforms-set-design-principles-develop-comprehensive-pcve.

[18] Aoife Gallagher, Ciarán O'Connor, Pierre Vaux, Elise Thomas, and Jacob Davey, *Gaming and Extremism: The Extreme Right on Discord*, Institute for Strategic Dialogue (2021), https://www.isdglobal.org/isd-publications/gaming-and-extremism-the-extreme-right-on-discord/; Daniel Koehler, Verena Fiebig, and Irina Jugl, "From Gaming to Hating: Extreme-Right Ideological Indoctrination and Mobilization for Violence of Children on Online Gaming Platforms," *Political Psychology* 44, no. 2 (2023): 419–34, https://doi.org/10.1111/pops.12855; Jens F. Binder and Jonathan Kenyon, "Terrorism and the Internet: How Dangerous Is Online Radicalization?" *Frontiers in Psychology* 13 (2022): 997390, https://doi.org/10.3389/fpsyg.2022.997390.

[19] M. R. Leiser, "Protecting Children from Dark Patterns and Deceptive Design," *SSRN Scholarly Paper* (2023), https://papers.ssrn.com/abstract=4660222.

[20] Fairplay,"Designing for deception: How the tech industry uses dark patterns to discourage privacy-protective behavior," 2021, https://fairplayforkids.org/wp-content/uploads/2021/05/darkpatterns.pdf.

[21] Information Commissioner's Office, "Introduction to the Children's Code," *Information Commissioner's Office Website,* 2023, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/introduction-to-the-childrens-code/; Information Commissioner's Office,"Children Are Better Protected Online in 2022 than They Were in 2021" - ICO Marks Anniversary of Children's Code," *Information Commissioner's Office Website*, ICO, 24 October, 2022, https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/children-are-better-protected-online-in-2022-than-they-were-in-2021/.

[22] Harvard Graduate School of Education, 2023, "How to Support Your Child's Digital Life," 13 March, 2023, https://www.gse.harvard.edu/ideas/edcast/23/03/how-support-your-childs-digital-life.

[23] Information Commissioner's Office,"Children Are Better Protected Online in 2022 than They Were in 2021" - ICO Marks Anniversary of Children's Code," *Information Commissioner's Office Website*, ICO, 24 October, 2022, https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/children-are-better-protected-online-in-2022-than-they-were-in-2021/.

[24] Phil Muncaster, "US Sues TikTok For Children's Law Violations," *Infosecurity Magazine* (5 August 2024), https://www.infosecurity-magazine.com/news/us-sues-tiktok-for-childrens-law/.

[25] Heidi Schulze, Simon Greipl, Julian Hohner, and Diana Rieger, "Social Media and Radicalization: An Affordance Approach for Cross-Platform Comparison," *Medien & Kommunikationswissenschaft* 72 (1 January 2024): 187–212, https://doi.org/10.5771/1615-634X-2024-2-187.

[26] Katerina Vittozzi, "Sharp Rise in Children Investigated over Far-Right Links - Including Youngsters under 10," Sky News, 24 November , 2020, https://news.sky.com/story/sharp-rise-in-children-investigated-over-far-right-links-including-youngsters-under-10-12131565.

[27] Lola Okolosie,"Parents, Talk to Your Sons about Andrew Tate – We Teachers Can't Take Him on Alone," *The Guardian*, 14 February , 2023, sec. Opinion, https://www.theguardian.com/commentisfree/2023/feb/14/parents-sons-andrew-tate-teachers-toxic-influencers; Ben Quinn, "Rapid Rise' in Andrew Tate-Related Cases Referred to Prevent by Schools," *The Guardian*, 12 February , 2023, sec. UK news, https://www.theguardian.com/uk-news/2023/feb/12/rapid-rise-in-andrew-tate-related-cases-referred-to-prevent-by-schools.

[28] Lola Okolosie, "Parents, Talk to Your Sons about Andrew Tate – We Teachers Can't Take Him on Alone," *The Guardian*, 14 February , 2023, sec. Opinion, https://www.theguardian.com/commentisfree/2023/feb/14/parents-sons-andrew-tate-teachers-toxic-influencers.

[29] Ben Quinn "Rapid Rise' in Andrew Tate-Related Cases Referred to Prevent by Schools" *The Guardian*, 12 February , 2023, sec. UK news, https://www.theguardian.com/uk-news/2023/feb/12/rapid-rise-in-andrew-tate-related-cases-referred-to-prevent-by-schools.

[30] Cécile Rousseau, Diana Miconi, Janique Johnson-Lafleur, Christian Desmarais, and Ghayda Hassan, "Children of Extremist Parents: Insights from a Specialized Clinical Team,".*Clinical Child Psychology and Psychiatry* 29, no. 2 (2024): 687–99, https://doi.org/10.1177/13591045231192340; Michael Wolfowicz,Badi Hasisi, and David Weisburd, "What Are the Effects of Different Elements of Media on

Radicalization Outcomes? A Systematic Review," *Campbell Systematic Reviews* 18, no. 2 (2022): e1244, https://doi.org/10.1002/cl2.1244; Daniel Koehler, "Violent Extremism, Mental Health and Substance Abuse among Adolescents: Towards a Trauma Psychological Perspective on Violent Radicalization and Deradicalization," *The Journal of Forensic Psychiatry & Psychology* 31, no. 3 (2020): 455–72, https://doi.org/10.1080/14789949.2020.1758752.

31 Ines von Behr,Anais Reding, Charlie Edwards, and Luke Gribbon,"Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism," RAND Corporation, 2013, https://www.rand.org/pubs/research_reports/RR453.html.

32 Lise Waldek, Julian Droogan, and Catharine Lumby,*Feeling Terrified? The Emotions of Online Violent Extremism*, Elements in Histories of Emotions and the Senses (Cambridge New York, NY Port Melbourne New Delhi Singapore: Cambridge University Press, 2021).

33 Sonia Livingstone, Lucyna Kirwil, Cristina Ponte, and Elisabeth Staksrud, "In Their Own Words: What Bothers Children Online?" *European Journal of Communication* 29, no.3 (2014): 271–88, https://doi.org/10.1177/0267323114521045.

34 Radicalisation Awareness Network, "Digital Literacy for Practitioners: Inspiration from Youth Work," RAN Webinar Readouts. European Commission, 2022, https://home-affairs.ec.europa.eu/system/files/2023-02/ran_readout_digital_literacy_for_practitioners–inspiration_from_youth_work_14122022_en.pdf; Radicalisation Awareness Network, "Integrating the Online Dimension into Offline Pedagogical Practices," RAN Conclusion Paper, European Union Commission, 2022, https://home-affairs.ec.europa.eu/system/files/2022-06/ran_y-e_integrating_online_dimension_into_offline_pedagogical_practices_8-9032022_en.pdf.

35 Cécile Rousseau, Diana Miconi, Rochelle L. Frounfelker, Ghayda Hassan, and Youssef Oulhote, "A Repeated Cross-Sectional Study of Sympathy for Violent Radicalization in Canadian College Students," *The American Journal of Orthopsychiatry* 90, no. 4 (2020): 406–18, https://doi.org/10.1037/ort0000444.

36 Radicalisation Awareness Network, "The Role of Hotbeds of Radicalisation," RAN Conclusion Paper, European Commission, 2020, https://home-affairs.ec.europa.eu/system/files/2021-01/ran_small_scale_meeting_hotbeds_conclusion_en.pdf; Moonshot,"Extremism Across the Online Gaming Ecosystem," 2024, https://moonshotteam.com/resource/extremism-across-the-online-gaming-ecosystem/; Galen Lamphere-Englund and Jessica White, "The Online Gaming Ecosystem: Assessing Digital Socialisation, Extremism Risks and Harms Mitigation Efforts," Global Network on Extremism and Terrorism, 2023, https://doi.org/10.18742/pub01133.

37 Radicalisation Awareness Network, "Integrating the Online Dimension into Offline Pedagogical Practices," RAN Conclusion Paper, European Commission, 2022b, https://home-affairs.ec.europa.eu/system/files/2022-06/ran_y-e_integrating_online_dimension_into_offline_pedagogical_practices_8-9032022_en.pdf; Menso Hartgers and Eviane Leidig, "Fighting Extremism in Gaming Platforms: A Set of Design Principles to Develop Comprehensive P/CVE Strategies," International Centre for Counter-Terrorism – ICCT, 1 June , 2023, https://www.icct.nl/publication/fighting-extremism-gaming-platforms-set-design-principles-develop-comprehensive-pcve.

38 Elizabeth D.Kilmer and Rachel Kowert, "Grooming for Violence: Similarities Between Radicalisation and Grooming Processes in Gaming Spaces,"*GNET* (2024), https://gnet-research.org/2024/02/08/grooming-for-violence-similarities-between-radicalisation-and-grooming-processes-in-gaming-spaces/ (January 24, 2025).

39 Brian Ballsun-Stanton, Lise Waldek, Julian Droogan, Debra Smith, Muhammad Iqbal, and Mario Peucker, "Mapping Networks and Narratives of Online Right-Wing Extremists in New South Wales," Zenodo, 2020, https://doi.org/10.5281/ZENODO.4071472.

40 United Nations Office on Drugs and Crime, 2017, "Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System," Vienna, Austria: United Nations, 2017, https://www.unodc.org/documents/justice-and-prison-reform/Child-Victims/Handbook_on_Children_Recruited_and_Exploited_by_Terrorist_and_Violent_Extremist_Groups_the_Role_of_the_Justice_System.E.pdf; Marc-André Argentino, Barrett G, and M.B. Tyler, "764: The Intersection of Terrorism, Violent Extremism, and Child Sexual Exploitation," *GNET* (blog), 19 January , 2024, https://gnet-research.org/2024/01/19/764-the-intersection-of-terrorism-violent-extremism-and-child-sexual-exploitation/.

41 Menso Hartgers and Eviane Leidig, "Fighting Extremism in Gaming Platforms: A Set of Design Principles to Develop Comprehensive P/CVE Strategies"; Flora Khoo and Brown William, "No Child's Play: IS Propaganda Videos and the Recruitment of Children," *GNET* (blog), 23 March , 2021, https://gnet-research.org/2021/03/23/no-childs-play-is-propaganda-videos-and-the-recruitment-of-children/.

42 Nick Robinson and Joe Whittaker, "Playing for Hate? Extremism, Terrorism, and Videogames," *Studies in Conflict & Terrorism* (2021): 1–36, https://doi.org/10.1080/1057610X.2020.1866740.

[43] United Nations Meetings Coverage and Press Releases, “Stop Feeding Terrorism with Blood of Our Youth,’ Jordan’s Crown Prince Tells Security Council during Debate on Violent Extremism,” 23 April , 2015, https://press.un.org/en/2015/sc11872.doc.htm; Nick Robinson and Joe Whittaker, “Playing for Hate? Extremism, Terrorism, and Videogames”

[44] Allison Smith, “How Radicalization to Terrorism Occurs in the United States: What Research Sponsored by the National Institute of Justice Tells Us,” United States: National Institute of Justice (United States Department of Justice), 2018, https://www.ojp.gov/pdffiles1/nij/250171.pdf; Randy Borum and Terri D. Patterson,“Juvenile Radicalization into Violent Extremism: Investigative and Research Perspectives,” *Journal of the American Academy of Child & Adolescent Psychiatry* 58, no. 12 (2019): 1142–48, https://doi.org/10.1016/j.jaac.2019.07.932.

[45] Daniel Koehler, Verena Fiebig, and Irina Jugl, “From Gaming to Hating: Extreme-Right Ideological Indoctrination and Mobilization for Violence of Children on Online Gaming Platforms.”

[46] Ibid.

[47] Ibid.

[48] Gabbiadini, Alessandro, and Paolo Riva. ‘The Lone Gamer: Social Exclusion Predicts Violent Video Game Preferences and Fuels Aggressive Inclinations in Adolescent Players’. *Aggressive Behavior* 44, no. 2 (2018): 113–24. https://doi.org/10.1002/ab.21735;Plaisier, Xanthe S., and Elly A. Konijn. ‘Rejected by Peers—Attracted to Antisocial Media Content: Rejection-Based Anger Impairs Moral Judgment among Adolescents’. *Developmental Psychology* 49, no. 6 (2013): 1165–73. https://doi.org/10.1037/a0029399.

[49] Daniele Valentini, Anna Maria Lorusso, and Achim Stephan,“Onlife Extremism: Dynamic Integration of Digital and Physical Spaces in Radicalization,” *Frontiers in Psychology* 11 (2020), https://www.frontiersin.org/articles/10.3389/fpsyg.2020.00524.

[50] Sue Caton and Roderick Landman, “Internet Safety, Online Radicalisation and Young People with Learning Disabilities,” *British Journal of Learning Disabilities* 50, no. 1 (2022): 88–97, https://doi.org/10.1111/bld.12372.

[51] Kara Brisson-Boivin, “Young Canadians Pushing Back Against Hate Online,” MediaSmarts, 2019, https://mediasmarts.ca/.

[52] MPFS. 2022. “JIM-Studie 2022: Basisuntersuchung Zum Medienumgang 12- Bis 19-Jähriger.” Germany: Medienpädagogischer Forschungsverbund Südwest. https://www.mpfs.de/studien/jim-studie/2022/.

[53] Livingstone, Sonia, Lucyna Kirwil, Cristina Ponte, and Elisabeth Staksrud, ‘In Their Own Words: What Bothers Children Online?’

[54] Ibid.

[55] Kara Brisson-Boivin, “Young Canadians Pushing Back Against Hate Online.”

[56] Royal Canadian Mounted Police,, “Five-Eyes Insights – Young People and Violent Extremism: A Call for Collective Action,” *Royal Canadian Mounted Police*, 2024, https://rcmp.ca/en/corporate-information/publications-and-manuals/five-eyes-insights-young-people-and-violent-extremism-call-collective-action(January 24, 2025).

[57] Virginia Braun, and Victoria Clarke,*Thematic Analysis: A Practical Guide to Understanding and Doing* (London ; Thousand Oaks, California: Sage Publications Ltd, 2021).

[58] Elisabeth Staksrud and Sonia Livingstone, “CHILDREN AND ONLINE RISK: Powerless Victims or Resourceful Participants?” *Information, Communication & Society* 12, no. 3 (2009): 364–87, https://doi.org/10.1080/13691180802635455; Elizabeth A.Vandewater, Victoria J. Rideout, Ellen A. Wartella, Xuan Huang, June H. Lee, and Mi-suk Shim, “Digital Childhood: Electronic Media and Technology Use Among Infants, Toddlers, and Preschoolers,” *Pediatrics* 119, no. 5 (2007): e1006–15, https://doi.org/10.1542/peds.2006-1804.

[59] Kowert, Rachel, Alexi Martel, and William B. Swann. ‘Not Just a Game: Identity Fusion and Extremism in Gaming Cultures’. *Frontiers in Communication* 7 (17 October 2022): 1007128. https://doi.org/10.3389/fcomm.2022.1007128.

[60] K. Davis, *The two-step decision tool for digital parenting: Part 1 – Young children | Katie Davis*, 3 January, 2023), https://katiedavisresearch.com/blog/the-two-step-decision-tool-for-digital-parenting-part-1-young-children/.

[61] In this article, parasocial relationships are one-sided, imagined connections that distant observers form with public figures. In this type of relationship and in the context of online extremism, the child may feel a personal bond – feeling like they know them well, have shared personal experiences with

them, or have a deep understanding of their life – even though this bond is entirely one-sided. This sense of intimacy and connection is enabled by the digital media's portrayal of the public figure's life, enabling the children to feel a sense of familiarity and closeness.

62 Daniel Koehler,Verena Fiebig, and Irina Jugl, "From Gaming to Hating: Extreme-Right Ideological Indoctrination and Mobilization for Violence of Children on Online Gaming Platforms."

63 UNESCO, *Youth led guide on prevention of violent extremism through education*, UNESCO Digital Library, 2017, https://unesdoc.unesco.org/ark:/48223/pf0000260547.

64 Dr Jordan Peterson is a Canadian psychologist, author, and professor emeritus at the University of Toronto. He gained international prominence in 2016 for his opposition to compelled speech legislation in Canada, particularly Bill C-16, which added gender identity and gender expression to the list of prohibited grounds of discrimination. Peterson's lectures and debates on cultural and political issues have garnered millions of views on platforms like YouTube, where he discusses topics such as free speech, political correctness, and identity politics. His self-help books '12 Rules for Life: An Antidote to Chaos' and then 'Beyond Order' became bestseller popular trade books, resonating with a wide audience for its advice on personal responsibility and finding meaning in life. However, Peterson's views have also sparked significant controversy, with critics accusing him of promoting misogyny, transphobia, and conservative ideology under the guise of academic rigor. His opposition to contemporary social justice movements and critiques of feminism and identity politics have polarised public opinion, making him a highly influential yet contentious figure in modern discourse.

65 Tim Lott, "Jordan Peterson and the Transgender Wars," *The Spectator*, 20 September, 2017, https://www.spectator.co.uk/article/jordan-peterson-and-the-transgender-wars/; Tim Lott, "Jordan Peterson: "The Pursuit of Happiness Is a Pointless Goal,"" *The Observer*, 21 January, 2018, sec. Global, https://www.theguardian.com/global/2018/jan/21/jordan-peterson-self-help-author-12-steps-interview; Dorian Lynskey, "How Dangerous Is Jordan B Peterson, the Rightwing Professor Who "Hit a Hornets" Nest'?" *The Guardian*, 7 February, 2018, sec. Science, https://www.theguardian.com/science/2018/feb/07/how-dangerous-is-jordan-b-peterson-the-rightwing-professor-who-hit-a-hornets-nest; Kelefa Sanneh, "Jordan Peterson's Gospel of Masculinity," *The New Yorker*, 26 February, 2018, https://www.newyorker.com/magazine/2018/03/05/jordan-petersons-gospel-of-masculinity.

66 Daveed Gartenstein-Ross, and Madeleine Blackman, "Fluidity of the Fringes: Prior Extremist Involvement as a Radicalization Pathway," *Studies in Conflict & Terrorism* (2019): 1–24, https://doi.org/10.1080/1057610X.2018.1531545.

67 Daveed Gartenstein-Ross and Madeleine Blackman, "Fluidity of the Fringes: Prior Extremist Involvement as a Radicalization Pathway."; Boraz Ganor, "Terrorism Is Terrorism: The Christchurch Terror Attack from an Israeli CT Perspective," Event Report, Special Report, Australia: Australian Strategic Policy Institute, 2020, https://www.aspi.org.au/report/terrorism-terrorism-christchurch-terror-attack-israeli-ct-perspective.

68 Siege Culture represents an extreme interpretation of fascism and national socialism, characterised by anti-democratic, anti-enlightenment, racist, and white supremacist beliefs (see Johnson & Feldman, 2021).

69 Bethan Johnson and Matthew Feldman, "Siege Culture After Siege: Anatomy of a Neo-Nazi Terrorist Doctrine," *ICCT Research Paper* (2021), https://doi.org/10.19165/2021.1.07

70 Craig A. Andersonand Brad J. Bushman, "Media Violence and the General Aggression Model," *Journal of Social Issues* 74, no. 2 (2018): 386–413, https://doi.org/10.1111/josi.12275.

71 Daniel Koehler, Verena Fiebig, and Irina Jugl, "From Gaming to Hating: Extreme-Right Ideological Indoctrination and Mobilization for Violence of Children on Online Gaming Platforms."; Radicalisation Awareness Network, "Digital Grooming Tactics on Video Gaming & Video Gaming Adjacent Platforms: Threats and Opportunities," RAN Conclusion Paper, European Commission, 2021, https://home-affairs.ec.europa.eu/system/files/2021-05/ran_c-n_conclusion_paper_grooming_through_gaming_15-16032021_en.pdf.

72 Ghayda Hassan, Sébastien Brouillette-Alarie, Séraphin Alava, Divina Frau-Meigs, Lysiane Lavoie, Arber Fetiu, Wynnpaul Varela, et al., "Exposure to Extremist Online Content Could Lead to Violent Radicalization:A Systematic Review of Empirical Evidence," *International Journal of Developmental Science* 12, no. 1–2 (1 January 2018): 71–88, https://doi.org/10.3233/DEV-170233; Ghayda Hassan, Jihan Rabah, Pablo Madriaza, Sebastien Brouillette-Alarie, Eugene Borokhovski, David Pickup, Wynnpaul Varela, Melina Girard, Loïc Durocher-Corfa, and Emmanuel Danis, "PROTOCOL: Hate Online and in Traditional Media: A Systematic Review of the Evidence for Associations or Impacts on Individuals, Audiences, and Communities," *Campbell Systematic Reviews* 18, no. 2 (2022), https://ideas.repec.org//a/wly/camsys/v18y2022i2ne1245.html.

[73] Sébastien Brouillette-Alarie, Ghayda Hassan, Wynnpaul Varela, Sarah Ousman, Deniz Kilinc, Éléa Laetitia Savard, Pablo Madriaza, Shandon Harris-Hogan, John McCoy, Cécile Rousseau, Michael King, Vivek Venkatesh, Eugene Borokhovski and David Pickup,Systematic Review on the Outcomes of Primary and Secondary Prevention Programs in the Field of Violent Radicalization, *Journal for deradicalization*, *Spring, no.* 30 (2022): 117–168.

[74] Martin Nystrand, Lawrence L. Wu, Adam Gamoran, Susie Zeiser, and Daniel A. Long, "Questions in Time: Investigating the Structure and Dynamics of Unfolding Classroom Discourse, "*Discourse Processes* 35, no. 2 (2003): 135–98, https://doi.org/10.1207/S15326950DP3502_3.

[75] Martin Nystrand, Lawrence L. Wu, Adam Gamoran, Susie Zeiser, and Daniel A. Long, "Questions in Time: Investigating the Structure and Dynamics of Unfolding Classroom Discourse."

[76] Marlies Sas, Koen Ponnet, Genserik Reniers, and Wim Hardyns, "The Role of Education in the Prevention of Radicalization and Violent Extremism in Developing Countries," *Sustainability* 12, no. 6 (January 2020): 2320, https://doi.org/10.3390/su12062320.

[77] Wilson Hernández Varona, "Listening to Emilce and Pedro: Exploring the Subjective Constitutions of Teachers amid Violence," *Teaching and Teacher Education* 132 (2023): 104260, https://doi.org/10.1016/j.tate.2023.104260.

[78] Håvard Haugstvedt, "The Role of Social Support for Social Workers Engaged in Preventing Radicalization and Violent Extremism," *Nordic Social Work Research* 12, no. 1 (2022): 166–79, https://doi.org/10.1080/2156857X.2020.1806102.

[79] Education Law Center, *Equity and Diversity: Defining the Right to Education for the 21st Century*, Education Law Center, 28 February, 2023, https://edlawcenter.org/equity-and-diversity-defining-the-right-to-education-for-the-21st-century/.

[80] UNESCO, *Youth led guide on prevention of violent extremism through education*, UNESCO Digital Library, 2017, https://unesdoc.unesco.org/ark:/48223/pf0000260547.

[81] M. Taylor, A.Fudge, N. Mirriahi, and M. de Laat, *Use of Digital Technology in Education: Literature Review*, South Australian Department of Education, 2021, https://www.education.sa.gov.au/docs/ict/digital-strategy-microsite/c3l-digital-technologies-in-education-literature-review.pdf.

PERSPECTIVES ON TERRORISM

RESEARCH ARTICLE

# On Querdenken, Reichsbürger and the Patriotic Union: Exploring the Formation of an Anti-Government Extremist Network in Germany

Leoni Heyn*

Volume XIX, Issue 1
March 2025

ISSN: 2334-3745
DOI: 10.19165/2025.8743

**Abstract:** This article examines the digital convergence of distinct extremist milieus involved in the Patriotic Union's thwarted plot to overthrow the German government in December 2022. By specifically investigating the merging process of involved digital networks of the German Corona-protest and Sovereign Citizens milieu over time, this article analyses the event's broader implications for the German extremism landscape linked to the transnational evolution of anti-government extremism (AGE). Empirically, this study explores the relationship between issue-driven AGE (*Querdenken*) and ideologically driven AGE (*Reichsbürger*) by conducting a longitudinal network analysis of 785,865 Telegram messages from the attempted storming of the *Reichstag* (August 2020) until the events of December 2022. The analysis reveals a 25.6 percent overlap between Querdenken and Reichsbürger channels, indicating a formation process of a new small, yet notable AGE network. Further, the article finds that the highest spikes of convergence occur in intervals correlating with large-scale offline events, suggesting a feedback loop of offline encounters and online convergence. Thus, this study contributes not only to a dearth of literature on German-centred extremism and transnational debates on their changing nature reflected in the growing body of research on AGE. This study also offers empirical insights into group-level online radicalisation processes.

**Keywords:** online convergence, anti-government extremism, Querdenken, Reichsbürger, network analysis, radicalisation, social media

* *Corresponding author: Leoni Heyn, Kiel University. Email: lheyn@politik.uni-kiel.de*

# Introduction

December 2022 – "Patriotic Union stopped in violently bringing down crucial infrastructure and installing monarchist government!" Its outlandish tone notwithstanding, this headline refers to an alarmingly concrete plan by over 60 extremists with access to at least 300 firearms and 150,000 rounds of ammunition. Consequently, the foiled coup attempt placed Germany's extremist landscape in the international spotlight.[1] Of particular interest was the constellation of involved milieus. While the incident was primarily attributed to the *Reichsbürger,* an extremist milieu that denounces the Federal Republic of Germany as illegitimate, it also involved conspiracy believers and former leaders of the heterogenous[2] *Querdenken* ("lateral thinking") movement.[3] Querdenken emerged as a local protest initiative in opposition to COVID-19 containment policies, quickly evolving into a state-wide movement through the coordinated use of the instant messenger Telegram.[4] Although the German domestic intelligence service (*Verfassungsschutz*, BfV) began monitoring Querdenken after repeated calls for attacks on the state government online and their involvement in the attempted storming of the Reichstag (2020) offline,[5] research at the time predicted that the movement would lose its cause and support once pandemic restrictions ended.[6]

Despite substantial media attention, academic analyses of the attempted coup and its wider implications for Querdenken remain underexplored. The re-emerged body of literature on Anti-Government Extremism (AGE) contextualises the significance of this gap. Ever since the pandemic, political violence eschews established categories of extremism *transnationally*. AGE posits that the thwarted coup, as well as the attempted storming of the Reichstag, are indicators of those transnational shifts adjacent to the violent riots against government institutions in Washington, DC in 2021 or Brasília in 2023. All events are characterised by heterogeneous actors who are similarly entrenched in the online and offline domains, conspiracy theories, and pandemic-related anti-government animosity.[7] Despite a growing number of case studies on different expressions of this "slippery […] concept", our theoretical and empirical understanding of different forms and their relations is still limited.[8]

This study seeks to advance this understanding by interpreting the attempted storming of the German Reichstag and the prevented coup plot of December 2022 as expressions of AGE. By analysing the relationship of therein involved online communities of Querdenken and Reichsbürger over time, I aim to also address the coup's wider implications: *To what extent does the coup reflect the formation process of a new online AGE network encompassing the digital convergence of issue-driven AGE (Querdenken) and ideologically driven AGE (Reichsbürger)?* In addition to refining AGE subcategories, this approach has the potential to help understand the perseverance and transformation of issue-driven movements beyond their respective issue, adding a granular perspective to research on the evolution of the far right.

Accordingly, this article begins to address the theoretical gap by proposing a framework to model the relationship of issue-driven (Querdenken) and ideological-driven (Reichsbürger) AGE. To empirically advance our understanding of this hybrid online/offline phenomenon, I perform a three-step network analysis of 785,865 Telegram messages: First, I compare the aggregated Telegram networks of Querdenken and Reichsbürger between 2020-2022 to establish a baseline understanding of issue and ideological AGE networks online. Second, to assess their level of convergence over this timeframe, I calculate their overall node overlap. To investigate the procedural evolution of this AGE network until the coup attempt, I lastly calculate the overlap for ten intervals pertinent to Querdenken's polarisation or the Patriotic Union's plotting from 2020 to 2022.

## Literature Review: Querdenken, Reichsbürger, and the Patriotic Union as Anti-Government Extremist Networks?

Two strands of literature inform our current knowledge of the subject: (1) German-centred extremism literature, and (2) the re-emerged transnational discipline of AGE. By integrating both strands, I aim to address their gaps for their mutual benefit. While AGE offers a nuanced perspective on German academic discourse of extremism, the analysis of Querdenken and Reichsbürger as examples of AGE helps clarify this "incomplete constellation of concepts […] to better understand and explain extremist phenomena."[9]

### *The German Angle*

Following the attempted storming of the Reichstag, the German Offices for the Protection of the Constitution began monitoring the pandemic-driven protests surrounding Querdenken. In 2021, their observations led to the creation of a new category called "delegitimisation of the state relevant to the protection of the constitution."[10] Despite this, academic literature in Germany focuses largely on Querdenken from a sociological or social movement perspective, leaving a gap in understanding its extremist factions. Early surveys from 2020/2021 initially highlighted the sociopolitical heterogeneity of protestors,[11] with some scholarship highlighting this "community of distrust's"[12] historical ties to life-reformerism and esotercism.[13] In most studies, reference was made to an "extremist potential",[14] although not being the focus of analysis. Goertz was among the first in 2022 to call for nuanced security-focused examination of Querdenken, pointing to its "complex mixture of radicalism, conspiracy theories, and extremism."[15]

This call remains timely, as the attempted storming of the Reichstag and the attempted coup continue to raise questions about Querdenken's radicalisation. While the attempted storming of the Reichstag is clearly recognised as indicative of this radicalisation,[16] scholarship has not yet fully addressed the overlapping impact of right-wing extremists, Querdenken, and Reichsbürger. In fact, different studies blame right-wing extremists,[17] Querdenken,[18] or Reichsbürger[19] respectively as primarily responsible for the incident. This ambiguity extends to the coup attempt intervened in December 2022.[20] However, the Patriotic Union has increased scholarly attention to Reichsbürger.[21] Moreover, little relation has so far been drawn between these events despite identified continuities in the involved personnel.[22] Several actors arrested in suspicion of plotting against the government lead by Reichsbürger and minor aristocrat Heinrich XIII were either part of the Querdenken movement or had strong ties to it.[23] One of them was Maximilian Eder, a former Bundeswehr colonel who regularly spoke at Querdenken demonstrations and is said to be in contact with leaders of the movement like Michael Ballweg or Markus Haintz.[24]

Policy papers highlight that the movement seems to be adapting to new incidents.[25] Still, some scholars predicted that Querdenken, as a social movement, would lose its cause and support post-pandemic.[26] Heinke explains why this might not be the case for the extremist factions of Querdenken: "The threat posed by the movement is that it can fuel anti-government sentiments" which may lead to a radicalisation of fractions into a "violent anti-government ideology."[27] The relevance of the case of 2022 thus lays in its illustrative potential of the development of Querdenken: *Is the subjunctive act of plotting to overthrow the government of Reichsbürger and Querdenker proof for the ongoing radicalisation of Querdenken or even a merging process with the Reichsbürger movement?*

Despite the recognition of shared anti-government attitudes, interpersonal ties and shared interaction spaces on social media between Querdenken and Reichsbürger,[28] insights into their convergence are scant. The intersection of both milieus with digital platforms introduces another layer of complexity to this gap. Querdenken emerged as a hybrid online/offline movement, heavily and effectively relying on Telegram to mobilise and organise demonstrations.[29] Reichsbürger, like many extremist movements, capitalised on this hybridity by expanding their presence in the digital domain, seeking to co-opt the movement.[30] This tactic proved effective; Telegram became a sight of radicalisation and increased interaction with other extremist movements.[31] The network analysis by Zehring and Domahidi illustrates that Querdenken predominantly forwards content from far-right and QAnon channels. However, empirical studies on these online interactions remain limited, and a comprehensive understanding of the digital convergence between Querdenken and Reichsbürger is still lacking.

## *Fusing Anti-Government Extremism and German Extremism Studies?*

A part in this lack of clarity has the tendency to subsume Querdenken and Reichsbürger under the umbrella terms "far-right," "right-wing extremism," or "new right" in German academic and political discourse. This is not only problematic, as a lack of understanding impedes effective countermeasures,[32] but also because the label of right-wing extremism potentially obscures the evolving nature of extremism since the onset of the pandemic. Mackenzie and Kaunert note that research on right-wing extremism in 2024 faces "diverse challenges" including "subcultural movements, such as the Reichsbürger", pandemic exploitation, a "fluid participation in ostensibly different scenes", and "stronger transnational connections".[33] A large body of quantitative longitudinal analyses shows that these observations are illustrative of two transnational trends within the domain of extremism: 1) global shifts towards anti-government sentiments, especially since the pandemic,[34] and 2) a fragmentation and remixing of (extremist) ideologies, especially online.[35] Within the digital sphere, both trends are heavily interlinked, fuelling continued prevalence after the pandemic.[36]

Therefore, this study aims to enhance German-centred extremism literature by offering a transnational and nuanced perspective on Querdenken and Reichsbürger through the lens of AGE. Querdenken, Reichsbürger, and notably the coup plotters of the Patriotic Union, demonstrate strong narrative adaptations and hybrid interconnections with the transnational QAnon conspiracy movement, akin to other AGE-labelled events such as January 6th in Washington, DC.[37]

The integration of the German events within the transnational trends also allows for a more nuanced understanding of Querdenken and Reichsbürger. Jackson asserts that AGE is characterised by a sustained and primary opposition to government entities, perceived as the root cause of crisis. He further differentiates AGE into the distinct forms of "issue-driven" and "ideological driven", which case studies have successfully utilised to investigate COVID-19 protestors in the Netherlands and Australia, or Sovereign Citizens globally.[38] For instance, Rathje or van der Buuren used the ideological-driven frame to explain the ideological reliance of Sovereign Citizens on conspiracy theories or sovereignism.[39] Of particular relevance to this article is the work of Hartleb, Schliefsteiner, and Schiebel, who argued for a connection between Querdenken and Reichsbürger based on shared conspiracy theories.[40]

While this highlights the usefulness of the AGE framework for a more granular understanding of Querdenken and Reichsbürger, the relationship between issue-driven and ideological-driven AGE has neither been fully conceptualised, nor empirically investigated in the digital realm. This gap is especially significant given the increasing reliance on digital platforms, such as Telegram, for mobilisation and radicalisation. Thus, the second noteworthy contribution of the case of the Patriotic Union lays in its potential to clarify definitional ambiguities of AGE, allowing for a specification of the question: *To what extent does the coup reflect the formation process of a new online AGE network encompassing the digital convergence of issue-driven AGE (Querdenken) and ideologically driven AGE (Reichsbürger)?*

## Theory: Understanding the Relationship between Issue-Driven and Ideologically Driven AGE

To evaluate the developments from the storming of the Reichstag to the attempted coup as indicative of a nascent extremist network, it is imperative to first delineate which definitional characteristics ought to be met. Integrating Jackson's argument with Khalil and Roose's observations, I contend that the emergence of AGE depends on a core manifestation of anti-government animosity, fuelled by conspiracy theories, a heavy social media utilisation, and shared grievances.[41] While these factors work in conjunction, their timely contextualisation may accelerate the process. Fischer shows that the establishment of *Feindbilder*[42] (enemy images) depends on their resonation with pre-existing epistemological frameworks (i.e. conspiracy theories) and contemporary events (i.e. the pandemic), which in turn facilitates their potential to mobilise individuals.[43]

Also loosely drawing on Social Network and Social Movement Theory, I define an AGE network as a pattern of dynamic and rather informal relationships between heterogeneous actors that are connected by a varying degree of (a) anti-government sentiments, and (b) shared actors/social bonds.[44]

Given the focus of this study, I thus build an argument based on the following assumptions:

(1) **The formation of a network must be understood as a process of social and narrative interactions.** Acknowledging the formation as a process, it must be clear that the formation of a network is a phase of defining in-group membership between subgroups, resulting in inter- and intra-network barriers still being permeable and bound to fluctuations.[45] Therefore, this study explores the evolution of a dynamic interaction space rather than the establishment of a fully integrated extremist group in a traditional sense.

(2) **The attempted coup intervened in December 2022 is a result of the formation process**. This assumption is rooted in AGE literature labelling the coup plot as a central example for AGE,[46] thus a highly saturated process of AGE evolution. More specifically, the involvement of issue-driven individuals in a plot predominantly driven by ideological AGE may exemplify a highly saturated convergence of both into a single network. AGE network formation can thereby be evaluated by exploring the relationship of the involved AGE subgroups over time.

(3) **Querdenken and Reichsbürger represent different subgroups of AGE**. Jackson differentiates between "ideological anti-government extremism that is broadly opposed to government (or broadly opposed to particular governments) from issue-driven anti-government extremism that opposes a government because of that government's stance (or course of action) on an issue."[47] Reichsbürger, akin to Sovereign Citizens internationally, epitomise a primarily ideological AGE movement, fundamentally rejecting the legitimacy of the government. Conversely, Querdenken emerged as a protest movement primarily aimed at challenging pandemic containment measures, with some extremist factions serving as examples of issue-driven AGE.

(4) **The relationship between issue-driven AGE and ideological AGE is in its core context-dependent**: Molas et al. note that Reichsbürger are the most extreme form of AGE, and Goertz shows how Querdenken is most deeply intertwined with legal forms of political dissent.[48] Hence, there is a gap in the depth of anti-government sentiments or understanding of means deemed legitimate to act on these sentiments. Consequently, for issue-driven individuals to shift opposition in a "non-normative direction"[49] from issue to government fundamentally, at least some form of cognitive radicalisation occurs. In this context, "radicalization is fundamentally a group socialization process through which [issue-driven] people develop identification with a set of norms – that may be violent or non-violent – through situated social interactions […]."[50] These situated interactions, including both the social process and content, are comparable to political opportunity theory:[51] they are inseparable from the context of their appearance – thus the issue of anti-government sentiment.

In consequence of the definition outlined above, the two forms are generally linked by their epistemological structures of anti-government sentiment, anti-elitism, and conspiracy theories. It is these shared perspectives that can serve as the basis for cognitive and behavioural interaction between the two forms. Meiering et al. show that group-bridging narratives can not only structure patterns of perception but also clarify attributions of belonging and create shared opportunities for action.[52] Out of the three narratives, the shared anti-government sentiment acted as a catalyst to create shared opportunities for interactions, potentially fostering the radicalisation from issue-driven individuals to ideologically driven AGE.

In the case of Querdenken, issue-driven individuals were united by their collective sense of governmental injustice on the issue of pandemic containment. Due to perceived injustice or grievances individuals within protest groups may undergo a process of cognitive opening to more radical ideas, thereby triggering group level mechanisms of radicalisation via group polarisation over time.[53] According to McCauley and Moskalenko this potential for (in this case cognitive) radicalisation is the strongest when grievances are interpreted "in the context of a group and as part of a larger political struggle".[54]

Ideologically driven AGE has the potential to validate and shape this perception of political conflict. According to Hansen, the extremist factions that emerged during the pandemic protests in Germany are to be differentiated from other forms of extremism due to their failure to provide an alternative to the rejected political system.[55] Ideologically driven AGE provides this alternative. For example, in 2020, Michael Ballweg, a leading figure in the Querdenken movement, called for the creation of a new constitution, borrowing Reichsbürger arguments. He claimed that Germany needed a "peace treaty", lacked sovereignty, and therefore did not have a valid constitution.[56] Conversely, issue-driven AGE provides an opportunity for ideology-driven AGE to connect with a broader public that does not have ideological objections to the government.[57] This opportunity for recruitment also has a dualistic emotional appeal strengthening the interaction: issue-driven individuals feel seen in their perception of injustice, ideologically driven Reichsbürger feel heard in their rejection of the government.

Therefore, I propose to understand the relationship between issue-driven and ideological AGE as one of symbiotic opportunity that can sponsor processes of radicalisation of issue-driven individuals, potentially leading to group-level transformation or convergence with ideological forms of AGE over time. Thus, radicalisation is understood as a relational and social process mainly driven through means of interaction.[58]

The potential convergence of issue-driven towards ideologically driven extremism is, however, caveat to the specific characteristics of the German case and may not be applicable to other forms of issue-driven AGE.[59] The foundational values of Querdenken, such as the promotion of inclusivity, particularly create vulnerabilities to infiltration attempts by extremist actors seeking to co-opt the movement.[60] This openness can blur intergroup barriers, potentially paving the way for easier or larger-scale convergence with Reichsbürger. Pöhlmann highlights that this ethos is especially fuelled by a strive for harmony informed by esotericism.[61] In addition to conspiracy thinking and anti-government sentiments, esotericism is another bridging narrative rooted in Reichsbürger ideology, further lowering the boundaries for convergence.[62] In parallel to these group-bridging narratives, (opinion) leaders from the Querdenken scene actively established connection to the Reichsbürger scene: Hartleb, Schliefsteiner and Schiebel show that Michael Ballweg, Bodo Schiffmann or Attila Hildmann played a crucial role in spreading Reichsbürger narratives offline and, in their function as influencers, on their social media in the Querdenken sphere.[63]

In light of these dynamics, it is hypothesised that:

> **H**$_{1.1}$: The interaction between issue-driven and ideologically driven AGE, facilitated by shared actors and interaction spaces, culminates in the radicalisation of issue-driven individuals over time. This can potentially lead to group-level transformation or convergence with ideological forms of AGE.

With the following empirical implications:

> **H**$_{1.2}$: The higher the number of shared actors between issue-driven and ideologically driven individuals/accounts over time, the more likely is convergence into a new AGE network.

# Methods

## Study Design

The research design for this study is a combination of comparative network analysis and longitudinal node overlap analysis. First, I aim to differentiate the networks of issue-driven and ideological driven AGE by comparing two aggregated networks of Querdenken and Reichsbürger. Second, I assess the degree of convergence between the Querdenken and Reichsbürger movements by analysing longitudinal network data from Telegram. To do so, I utilised multiple seed lists derived from literature and reports by federal and state authorities, supplemented by snowball sampling. I then constructed weighted and directed network graphs to calculate the node overlap of two networks representing both Querdenken and Reichsbürger (a) overall, and (b) in ten intervals between August 2020 and December 2022, generated through mutual message forwarding.

## Sampling

Because there is relative agreement on the cross-milieu relevance of Telegram,[64] the platform is used as an access point to the field. However, sampling a dynamic, rather informal, and potentially clustered network on Telegram comes with a number of challenges.[65] Jost et al. highlight the need for a brief reflection that potentially resulting biases impact the sample composition and can shape direction of analyses. In this case, three characteristics of non-institutionalised movements on Telegram arise:[66]

(1) The ideological and structural heterogeneity of AGE leads to ambiguity in the identification of relevant actors.

(2) Sparse data on AGE means that the population is largely unknown.

(3) The large time lag between data collection and channel or message creation of respective actors implies blind spots for all deleted or deplatformed channels.[67]

To best circumvent these challenges in finding actors, I combined multiple seed lists with snowball sampling via link-based network techniques with both in-platform and external approaches, as suggested by Semenzin and Bainotti.[68]

### *Seed Lists*

While I acknowledge the third characteristic mentioned above as a limitation of my study, I derived inclusion and exclusion criteria for my seed list from the first and second characteristic. I excluded content-based sampling techniques, as due to the diversity of the field, no clear categorisation to either Reichsbürger or Querdenken is possible. Consequently, I have only included actors in the seed that can be strictly categorised as either Reichsbürger or Querdenken, based on previous findings. To best capture the extremist factions of both parties, I reviewed the annual reports of the federal domestic intelligence service (BfV) of 2020, 2021, and 2022, as well as all reports of Germany's sixteen states of 2021. I then coded the chapters for the respective observation categories with MAXQDA for named actors, entities, social media channels, or websites. This resulted in a list of 215 actors and their potential channels. To this list, I added all Querdenken-related channels (N=578) identified through similar sampling strategies by Zehring and Domahidi, and all Reichsbürger actors (N=19) monitored by CeMAS.[69] After I combined the lists for both Querdenken (N=631) and Reichsbürger (N=181), I dropped all duplicates and any channel that could not be clearly classified as either Querdenken or Reichsbürger based on channel description and message content, as well as definitions derived from coding the security reports. To find channels, I followed the in-platform approach of Semenzin and Bainotti.[70] The entity and keyword list served as a basis for identifying 139 public channels through the in-platform search bar. However, the composition of this second seed was unequal (Querdenken N = 97, Reichsbürger N = 42), implying a bias towards Querdenken-related actors. For the best comparison, I created a third seed for Querdenken in accordance with the seed size of the Reichsbürger list (N=43). I prioritised including all actors labelled as extremist by the BfV reports (N=25) and then equally filled the remaining spots with the most prominent, the most followed, and (disregarding size and reach) the most protest-related channels aiming to reflect the heterogeneity and spatial dispersion of the network. Thus, the third seed list encompasses 43 public channels for both Querdenken and Reichsbürger.

### *Snowball Sampling*

Again, referring to Semenzin and Bainotti, I systematically expanded the third seed based on the forwarding function within Telegram.[71] This suggests "[...] some overlap in terms of topic discussion between both, making the newly discovered channel similarly relevant to the analysis."[72] Additionally, this systematic expansion allowed for the sampling of actors not potentially aware of their observation by security services, which could implicate their public behaviour. For its operationalisation, I scraped a total of 785.865 messages between 1 August 2020 and 18 December 2022 via the Telegram API and the Telethon Python package integrated in 4CAT.[73]

## Data Analysis

To define the relationship between Querdenken and Reichsbürger, I initially built two weighted and directed network graphs for both entities, with nodes representing channels and edges forwarded messages aggregated over the two-year study period. I then conducted a three-step analysis. First, I broadly compared the structural characteristics of the two networks. Then, I calculated the aggregated node overlap between both networks assuming that shared actors indicate the level of convergence. To specify this development over time, I lastly defined ten monthly intervals relevant for the polarisation of the protest scene and the formation of the coup plotters (Table 1) and again calculated the overall node overlap for each interval.

*Table 1: Chosen monthly intervals for longitudinal node overlap analysis based on relevant events for either the protest-scene or the coup plotting entity Patriotic Union (PU)*

| No. | Interval | Event |
|---|---|---|
| 1 | Aug 2020 | Attempted Storming of the Reichstag |
| 2 | Nov 2020 | Leading figures of Querdenken (M. Ballweg) and Reichsbürger (P. Fitzek) meet |
| 3 | Apr 2021 | So-called „hard lockdown“ with stricter contact restrictions |
| 4 | Jul 2021 | Both exploit flood in Ahrtal for mobilisation. Initial meeting of PU |
| 5 | Oct 2021 | Core of PU meets repeatedly. Concrete plans are developed to storm the Bundestag |
| 6 | Feb 2022 | First meeting of PU to form a shadow cabinet at Reuss' Schloss Waidmannsheil |
| 7 | Apr 2022 | Arrest of another coup-plotting group, loosely connected to PU |
| 8 | Jul 2022 | End of containment policies. PU intensifies efforts to recruit personnel for their plans |
| 9 | Sep 2022 | Death of Queen Elisabeth is interpretated as sign by QAnon/PU to initiate plans |
| 10 | Nov 2022 | PU members demand that action be taking soon |

## Limitations

While the heavy reliance of both milieus on Telegram justifies the platform choice, it does not come without limitations. As noted at the beginning of this chapter, sampling a dynamic, informal and heterogenous pool of actors over time may come at the cost of under- or misrepresenting less active, inactive, or deplatformed accounts. As the inclusion of private accounts would further require ethically challenging field intervention and thus bias results, this study chooses to only sample public accounts. Given the fact, that it is in the best interest of extremists planning a coup to not be detected, this may exclude key actors.

However, as the trials are still ongoing and the perpetrators largely unknown, an attempted sampling of the Patriotic Union would be highly unethical. Rather, the sample composition aims to represent extremist-leaning accounts in the wider ideological information ecosystem of the Patriotic Union, which is more appropriate for a broader understanding of issue-driven and ideological AGE. In reference to the theoretical assumption, this study also understands the coup attempt as an indicator of highly saturated network convergence. As such, node overlap can only investigate this process, not prove its completion.

# Results

Here, I present my results for my research question evaluating the extent of convergence between ideologically driven AGE (Reichsbürger) and issue-driven AGE (Querdenken) to assess the formation of a new AGE network. To answer this question, I will start with a brief description of the aggregated networks of public channels (nodes) and therein forwarded channels (edges) for both Querdenken and Reichsbürger between 1 August 2020 and 18 December 2022. I then present the results for the node overlap in total and over time to assess the degree of convergence.

## Network Comparison

The weighted and directed network graphs for Reichsbürger (Figure 1) and Querdenken (Figure 2) will be broadly described along the three characteristics of network size and density, community structure, and communication activity.

First, in terms of network size and density, Querdenken emerges as the larger entity, boasting 3.717 nodes and 13.753 edges, in contrast to Reichsbürger's 3.342 nodes and 8.863 edges. This discrepancy suggests a denser and more interconnected communication structure within Querdenken, indicative of a potentially broader reach and influence within its network.

*Figure 1: Aggregated Network of Reichsbürger 2020-2022*

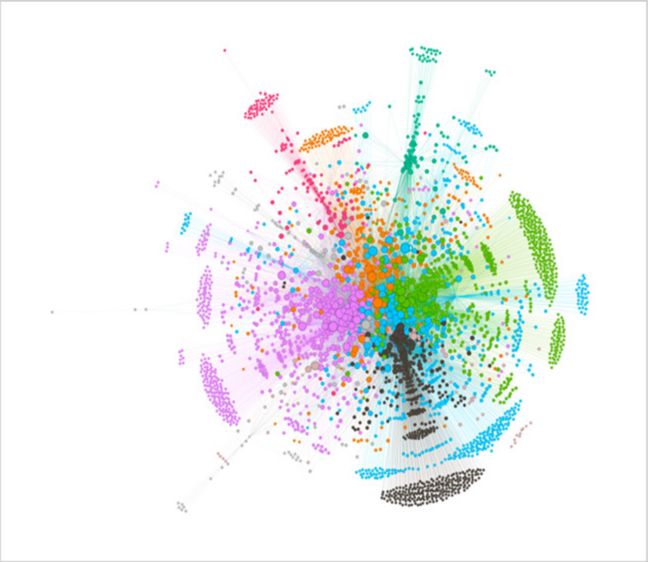
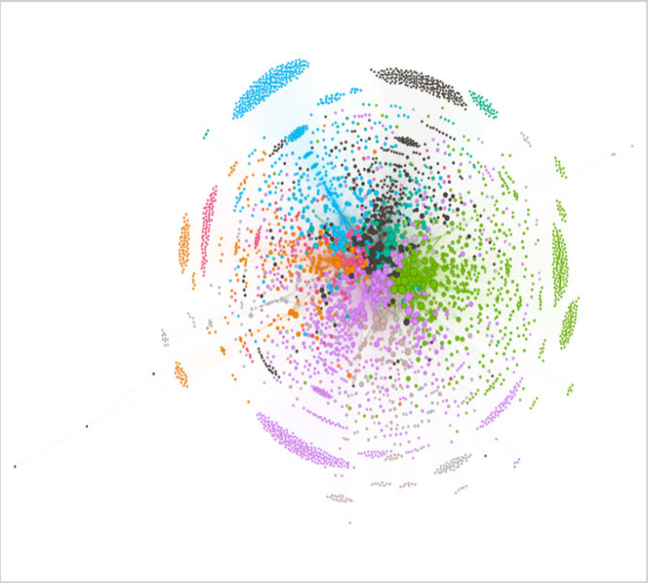


*Figure 2: Aggregated Network of Querdenken 2020-2022*



Second, the community structure within each network reveals only nuanced differences. As shown by the Louvain algorithms in Figure 1 and 2, both networks exhibit a community structure with nodes grouped into several distinct communities based on their communication patterns. The Reichsbürger network has slightly more communities (N = 14) than Querdenken (N = 13), while the communities are also slightly more evenly distributed in size. Consequently, this suggests a less evenly distributed community structure within Querdenken, with a higher concentration of nodes in the key communities.

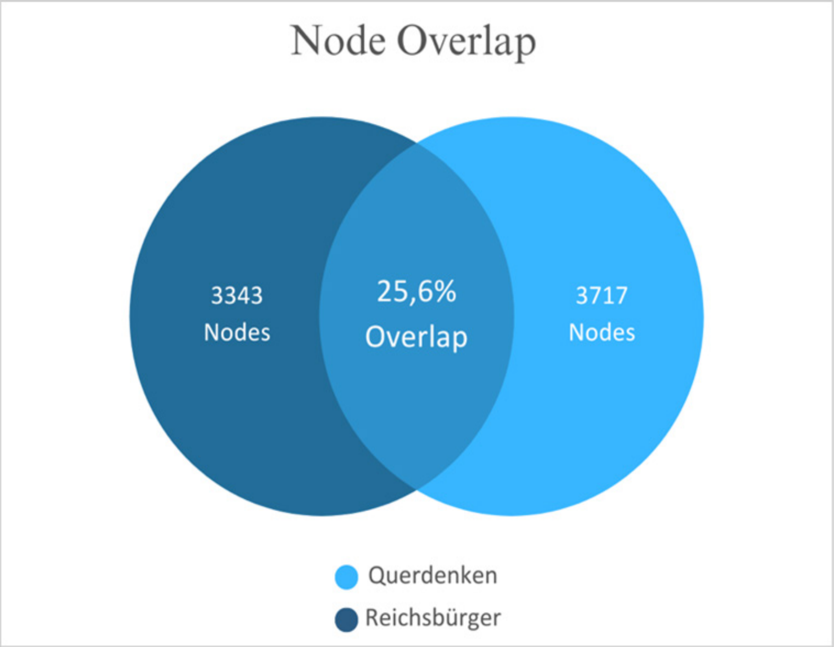
Third, the communication activity within the networks offers further insights. Despite having fewer nodes and edges, the Reichsbürger network demonstrates a higher total message count (N= 465.310) compared to Querdenken (N = 320.555). This heightened communication activity in the Reichsbürger network may signify a more focused or targeted approach to communication, potentially indicating greater coordination or engagement among members. Mirroring previous empirical observations, the ratio between messages and edges shows that Querdenken in comparison forwards more posts than actively writes itself.[74]

In interpretation, these findings underscore divergent organisational dynamics and communication patterns between the Querdenken and Reichsbürger networks. Querdenken appears to embody a more diffuse network structure, reflecting its heterogeneous membership base and varied ideological spectrum. In contrast, the Reichsbürger network exhibits a more cohesive and focused communication structure, characterised by more balanced community sizes and heightened communication activity. Finally, considering the topological network structure, the Reichsbürger cluster tend to be more spatially segregated, which may reflect the more established, yet more closed-off, self-proclaimed kingdoms or duchies.

## Node Overlap

The analysis of node overlap between the Querdenken and Reichsbürger networks over the period from August 2020 to December 2022 revealed several significant findings. The total overlap of 25.6 percent, representing 1.780 shared actors, indicates a notable level of convergence between the two groups (Figure 3).

*Figure 3: Node overlap between aggregated Querdenken and Reichsbürger networks 2020-2022*



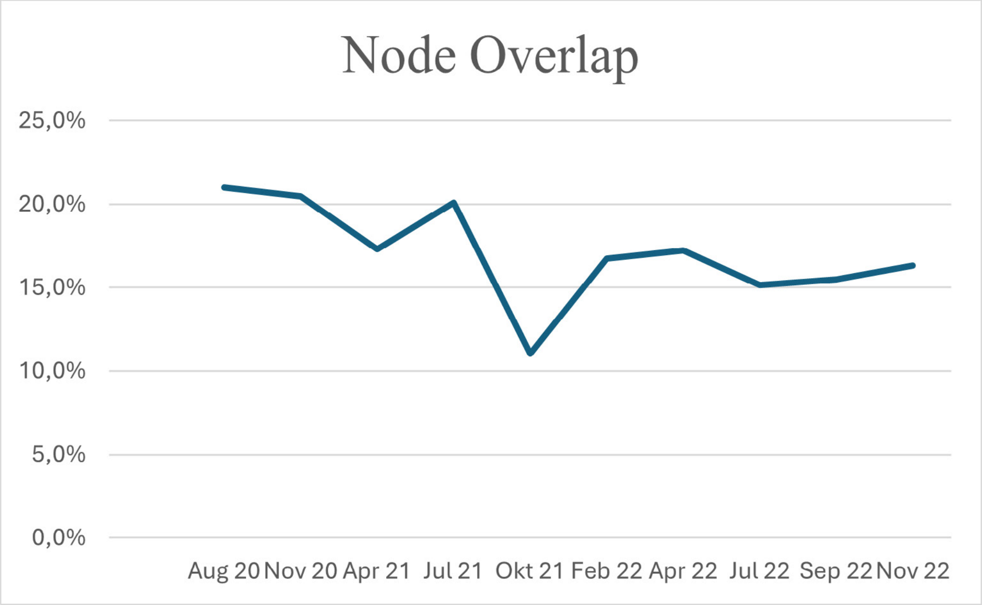
Further examination of the temporal development of the overlap, depicted in Figure 4, sheds light on the dynamics of the interaction between the Querdenken and Reichsbürger networks.

One notable observation is the slight decrease in overlap over time, which may signify several underlying trends. Firstly, the decline could potentially be attributed to a decrease in protest activity associated with Querdenken, possibly due to the perceived waning relevance of anti-COVID19 measures as the pandemic situation evolved. However, empirical evidence suggests that Querdenken's activity remained relatively stable, with consistent levels of engagement observed until February 2022.[75] This contradicts the hypothesis of decreased overlap due to decreased Querdenken activity. Another interpretation could relate to a polarisation effect, where less radical actors gradually disengage from the network over time.[76] However, given the steady rise in Querdenken activity and network expansion observed in previous research, this hypothesis warrants further investigation.[77]

The analysis also identified periods of peak and trough overlap between the two networks. High levels of overlap were observed in August and November 2020, July 2021, and April 2022, coinciding with significant real-world events such as the attempted storming of the Reichstag, the Ahrtal flood,[78] and the arrest of another coup-plotting group, loosely connected to the coup plotters around Prince Reuss through individual contacts.[79] Conversely, the lowest overlap occurred in October 2021, corresponding to a period with no significant demonstrations or public events facilitating interaction between the milieus. Interestingly, this interval was chosen because several secret meetings occurred in October between four core members of the AGE coup plotters of December 2022.[80]

Thus, these findings underscore the importance of larger-scale offline events as points of interaction for online convergence. They expand upon existing research, such as Schrimpf et al., who found a positive correlation between Querdenken's online mobilisation efforts and media coverage of demonstrations.[81] This suggests a potential feedback loop between online mobilisation and real-world events.

*Figure 4: Development of node overlap between Reichsbürger and Querdenken networks over ten monthly intervals*



In summary, the analysis of node overlap provides unexpected insights into the dynamics of the interaction between the Querdenken and Reichsbürger networks, highlighting the role of both online and offline factors in shaping the convergence of AGE movements.

## Discussion and Conclusion

In this paper, I interpreted the attempted storming of the Reichstag and the foiled coup of the Patriotic Union as instances of (German) AGE. I specifically analysed the extent of the coup's reflection on the formation of a new online AGE network comprising Querdenken and Reichsbürger, thereby aiming to understand the relationship between issue-driven and ideological AGE. To do so, I first proposed a theoretical framework for this relationship with specific attention to the characteristics of the German case. While I proposed to understand the relationship of issue-driven AGE and ideological AGE as one of symbiotic opportunity, I utilised a three-step network analytical approach to add empirical insights to my argument. Given the hybrid online/offline nature of AGE in general and the heavy reliance of both Querdenken and Reichsbürger on Telegram in particular, I scraped 785,865 Telegram messages from 43 public channel of each party to perform (1) a comparative network analysis, a node overlap analysis (2) overall and (3) in ten intervals.

### *Network Comparison*

The results of the network comparison provide valuable insights into the similarities and differences between issue-driven and ideological-driven AGE in the digital sphere. Taken together, the high message volume observed in both networks reinforces the hybrid nature of AGE,[82] demonstrating a heavy utilisation of Telegram. Known characteristics of both forms allow for further specification of their Telegram usage behaviour. While both networks exhibit heterogeneity, ideological-driven AGE appears to have a more established and cohesive structure with a higher message volume. This implies that ideological AGE uses Telegram mainly for communication and less for network expansion. To specify, Schuppener finds that Reichsbürger heavily engage in pseudo-legal discourse, aiming to justify and proof the illegitimacy of the Federal Republic of Germany.[83] In contrast, issue-driven AGE appears more diffuse with less balanced community sizes and fewer messages. In terms of Telegram usage, this may suggest that issue-driven AGE utilises Telegram to uphold their issue-specific mobilisation through network expansion, reflected in more edges. On their website, Querdenken outlines a specific channel set-up protocol to simplify expansion.[84] Thus fusing analyses of Querdenken as a social movement with network theory, this suggests that issue-driven AGE may have greater fluctuations and looser connections, but also a broader reach and influence due to its fluid nature.[85]

### *Node Overlap and Convergence*

The 25.6 percent node overlap between these networks indicates their partial convergence, enabling a formation process of a new smaller AGE online network between August 2020 and December 2022. Even though the overlap slightly decreases over time, it still illustrates the potential for issue-driven movements to transform within the AGE space. A key example is the peak in overlap in July 2021, where Querdenken adopted an entirely different issue – disaster management during the Ahrtal flood. This suggests that issue-driven movements, such as Querdenken, can evolve beyond their original cause by incorporating other grievances that resonate with and potentially deepen their anti-government narrative. Given that issue-driven AGE is sometimes hard to distinguish from legitimate forms of political dissent, this example exemplifies that it may be analytically useful to understand forms of AGE on a fluid spectrum rather than distinct categories.[86]

## *Context-Dependency and Hybridity for Convergence*

The variation in overlap over time and its correlation with significant large-scale offline events like the Ahrtal flood lends support to the hypothesis that interactions facilitated by shared actors and interaction spaces contribute to the radicalisation of issue-driven individuals over time, potentially leading to group-level transformation or convergence with ideological forms of AGE. More specifically, this finding underscores the assumption that the relationship between issue-driven and ideological AGE is in its core context-dependent. Their interaction and convergence is dependent on issues that stipulate large-scale mobilisation for both milieus and may be unrelated to the original cause of issue-driven movements. This insight is significant for two reasons.

First, it showcases a potential feedback loop between online and offline mobilisation and convergence, indicating empirical support for the "Onlife" radicalisation theory, where digital and real-world factors are seen as inseparable drivers for radicalisation.[87] However, while this mainly considers individual-level radicalisation, the correlation found here indicates that this theory may also apply for group-level radicalisation processes.

Second, the finding adds to our current understanding on the hybridity of AGE, a "predominantly online phenomenon with seldom expressions offline."[88] While the high message volume generally supports this, the *formation* of this online phenomenon seems heavily tied to (large-scale) offline expressions.

The findings may moreover specifically highlight the role of shared grievances and narratives in bridging the gap between issue-driven and ideology-driven AGE at those offline events: Renström, Bäck, and Knapton tested in four experiments to what extent individuals who face social exclusion (which is a common narrative of Querdenken) adapt to a radical including group. Three experiments were conducted online and one in a real-life setting. Only the last experiment showed the expected effect of social exclusion leading for "most people to endorse an extreme group."[89]

## *Contributions and Future Directions*

To conclude, this study makes three contributions to the literature. First, by integrating the body of AGE literature into German-centred extremism research, I provide a more nuanced understanding of Querdenken, Reichsbürger, and their interaction. Empirically, the comparative network approach highlights differences in communication patterns and organisational structures. Theoretically, contrasting these differences with their group-bridging similarities helps to understand their high ideological compatibility.

Second, by conceptualising issue-driven and ideological AGE within the same framework, this study advances the theoretical body of AGE. However, given the still limited literature on AGE, my theorising about the phenomenon comes with heuristic challenges, showcasing areas for future research: How can we best reflect upon a phenomenon that is transnational in nature but has country-specific anomalies? How can I contribute to conceptualising the relationship between issue-driven and ideological AGE when the very definition of issue-driven AGE as extremist is one of the biggest contested challenges? Since 2022, both Querdenken and Reichsbürger have incorporated pro-Russian narratives,[90] raising further theoretical and empirical questions about AGE milieus' role as as prosumers of disinformation and ideological realignment. Understanding AGE as an expression of broader shifts within extremism, this study lastly contributes to research on evolving group-level mobilisation and radicalisation pathways in the digital era, featuring less formal and more diffuse network-based milieus. My results revealed the critical role of online-offline interplay in the formation process of extremist networks, challenging monolithic approaches of monitoring and countering radicalisation. Consequently, counter-extremism strategies might find value in adopting hybrid approaches that synchronise large-scale offline events with corresponding digital spaces in real time.

*Leoni Heyn is a PhD candidate and researcher at both the Institute for Security Policy and the Department of Political Science at Kiel University. In her dissertation, she explores the formation and interconnectedness of German anti-government extremist networks (namely Reichsbürger, Querdenken, and QAnon) across different social media platforms.*

*Acknowledgements: The author thanks Jannis Jost and Jacqueline Dombrowski for countless helpful conversations and two anonymous reviewers for their valuable comments.*

# Endnotes

[1] To contextualise this recreated headline, in one of the biggest anti-terrorism operations in the modern history of Germany about 50 armed men and women were stopped in planning to overthrow the government. In order to take power, they intended to violently bring down crucial infrastructure to then install their previously selected government. For similar headlines compare i.e., Michael Götschenberg, Holger Schmidt, and Frank Bräutigam, „Bewaffnete Reichsbürger. Razzia wegen geplanten Staatsstreichs," *Tagesschau*, December 7, 2022, https://www.tagesschau.de/investigativ/razzia-reichsbuerger-staatsstreich-101.html; Vicky Isabelle Bargel, "Umsturzpläne von Reichsbürgern: "Es hätte sicher Tote gegeben"," *Zeit Online*, December 8, 2022, https://www.zeit.de/gesellschaft/zeitgeschehen/2022-12/reichsbuerger-umsturzplaene-staatsstreich-miro-dittrich; for further information on the plot and alleged perpertrators see i.e., Alexander Ritzmann, "The December 2022 German Reichsbürger Plot to Overthrow the German Government, " *CTC Sentinel* 16, no. 3 (2023): 15-20.

[2] They brought together a heterogeneous pool of sociopolitical milieus: green-alternative circles, esoteric-anthroposophical groups, fundamental Christians, conspiracy ideologists, but also more radical actors like Reichsbürger. However, for the sake of readability, in the following Querdenken will representatively refer to the protest scene. See further Florian Flinkbeiner, "Corona-Proteste, Verschwörungsmythen und Antisemitismus," *Demokratie-Dialog* 10 (2022): 51-59, https://doi.org/10.17875/gup2022-1944; Daniel Heinke, "The Security Threat Posed by the Corona-skeptic *Querdenken* Movement in Germany," *CTC Sentinel* 15, no. 3 (2022): 18-24.

[3] Ritzmann, "The December 2022 German Reichsbürger Plot."

[4] Tobias Schrimpf, Jan Dvorak, Andreas Reich and Jens Vogelgesang, "Aus dem Channel, auf die Straße! Wie die Querdenken-Bewegung ihren Protest auf Telegram organisiert – eine quantitative Netzwerkanalyse," *Medien & Kommunikationswissenschaft* 71, no. 3 (2023): 285-308, https://doi.org/10.5771/1615-634X-2023-3-4-285.

[5] Bundesministerium des Inneren und für Heimat (BMI), „Verfassungsschutzbericht 2021," (Berlin: Federal Ministry of the Interior and Community Germany, 2022), https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/vsb-2021-gesamt.html; Jan-Henrik Wiebe, "'Querdenker'-Szene. Täglich Tötungsaufrufe auf Telegram," *Tagesschau*, January 5, 2022, https://www.tagesschau.de/investigativ/funk/todesdrohungen-telegram-101.html.

[6] Boris Holzer, Sebastian Koos, Christian Meyer, Isabell Otto, Isabelle-Christine Panreck and Sven Reichardt, "Einleitung: Protest in der Pandemie," in *Die Misstrauensgemeinschaft der „Querdenker". Die Corona-Proteste aus kultur- und sozialwissenschaftlicher Perspektive*, ed. Sven Reichart (Frankfurt/New York: Campus Verlag, 2021), 7-26.

[7] Tore Bjørgo, "Introduction to the Special Section on Anti-Government Extremism," *Perspectives on Terrorism* 17, no. 1 (2023): 68, https://www.jstor.org/stable/27209218.

[8] Kurt Braddock and Tore Bjørgo, "Anti-Government Extremism: A New Threat?", *Perspectives on Terrorism*, 16, no. 6 (2022): 2, https://www.jstor.org/stable/27185087.

[9] Sam Jackson, "What Is Anti-Government Extremism?", *Perspectives on Terrorism*, 16, no. 6 (2022): 9, https://www.jstor.org/stable/27185088.

[10] Bundesministerium des Inneren und für Heimat (BMI), „Verfassungsschutzbericht 2021," (Berlin: Federal Ministry of the Interior and Community Germany, 2022), https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/vsb-2021-gesamt.html.

[11] Oliver Nachtwey, Robert Schäfer, and Nadine Frei, "Politische Soziologie der Corona-Proteste. Grundauswertung 17.12.2020," (Basel: Universität Basel), https://doi.org/10.31235/osf.io/zyp3f; Edgar Grande, Swen Hutter, Sophie Hunger, and Eylem Kanol, "Alles Covididioten? Politische Potenziale des Corona-Protests in Deutschland," *WZB Discussion Paper* 60, no. 1 (2021): 1-33, http://hdl.handle.net/10419/234470; Simon Teune, "Querdenken und die Bewegungsforschung – Neue Herausforderung oder déjà-vu?", *Forschungsjournal Soziale Bewegungen* 34, no. 2 (2021): 326-334.

[12] Holzer et al., "Einleitung: Protest," 18.

[13] Wolfgang Benz, *Querdenken. Protestbewegung zwischen Demokratieverachtung, Hass und Aufruhr* (Metropol-Verlag: Berlin, 2021); Reichardt, Die Misstrauensgemeinschaft; Malte Thießen, *Auf Abstand: Eine Gesellschaftsgeschichte der Corona-Pandemie* (Frankfurt: Campus Verlag, 2021); Gerhard Hanloser, "'Nicht rechts, nicht links'? Ideologien und Aktionsformen der 'Corona-Rebellen'," *Sozial.Geschichte Online,* no. 29 (2021): 175-217, https://sozialgeschichte-online.org/wp-content/uploads/2021/02/sgo_29_vorveroeffentlichung_hanloser_coronarebellen.pdf.

[14] Reference was made, for example, to the willingness of "some radical factions" to go beyond forms of legitimate protest in order to regain the freedom that they considered lost or to difficult patterns of interpretation that would enable the legitimisation of violence. See Teune, "Querdenken"; Holzer et al., "Einleitung: Protest."

[15] Goertz, Querdenker, 44.

[16] Sophia Hunger, Swen Hutter, and Eylem Kanol, "How Ideological Polarisation Drives Protest against Covid Containment Measures," *The Loop*, accessed May 2, 2023, https://theloop.ecpr.eu/how-ideological-polarisation-drives-protest-against-covid-containment-measures/.

[17] Decker, "Nach Sturm auf den Reichstag."

[18] Heinke, "The Security Threat."

[19] Keil, "Verschwörungserzählungen."

[20] Paul Kirby, "Germany arrests 25 accused of plotting coup," *BBC News*, December 7, 2022, https://www.bbc.com/news/world-europe-63885028.

[21] Dominik Juling, "Reichsbürger: An Old German Ideology in New Clothing?," in *Illiberalism Studies Program Working Papers*, no. 16 (2023), https://www.illiberalism.org/reichsburger-an-old-german-ideology-in-new-clothing/; Florian Hartleb, Paul Schliefsteiner, and Christoph Schiebel, "From Anti-Measure Activism to Anti-State Extremism? The 'Querdenker' Protest-Movement and Its Interrelation and Dynamics with the 'Reichsbürger' in Germany and Austria," *Perspectives on Terrorism* 17, no. 1 (2023): 123-144, https://www.jstor.org/stable/27209222; Barbara Horten and Marleen Orth, „Kriminologischer Beitrag: Politisch motivierte Kriminalität durch Reichsbürger und Selbstverwalter in der Bundesrepublik," *Forensische Psychiatrie, Psychologie, Kriminologie* 17, no. 2 (2023): 255-258, https://doi.org/10.1007/s11757-023-00771-x.

[22] Kirby, "Germany arrests 25"; Hartleb, Schliefsteiner and Schiebel, „From Anti-Measure to Anti-State"; Bundeskriminalamt (BKA) and BMI, "Politisch motivierte Kriminalität im Jahr 2022. Bundesweite Fallzahlen," (Berlin: Federal Ministry of the Interior and Community/Federal Criminal Police Office Germany, 2023), https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/nachrichten/2023/05/pmk2022-factsheets.pdf?__blob=publicationFile&v=5.

[23] Kirby, "Germany arrests 25."

[24] Simone Rafael, "Das breite Netzwerk der revolutionsbereiten Reichsbürger*innen," *Amadeu Antonio Stiftung*, 2022, accessed May 2, 2023, https://www.amadeu-antonio-stiftung.de/das-breite-netzwerk-der-revolutionsbereiten-reichsbuergerinnen-94091/.

[25] Amadeu Antonio Stiftung, "Energiekrise und Russlands Krieg. Das 'Querdenken'-Milieu als antidemokratische Kampagnenmaschine," *Amadeu Antonio Stiftung*, August 26, 2022, https://www.amadeu-antonio-stiftung.de/publikationen/energiekrise-und-russlands-krieg-das-querdenken-milieu-alsantidemokratische-kampagnenmaschine/.

[26] Holzer et al., "Einleitung: Protest."

[27] Heinke, "The Security Threat," 18.

[28] Matthias Pöhlmann, *Rechte Esoterik: Wenn sich alternatives Denken und Extremismus gefährlich vermischen* (Freiburg/Basel/Wien: Herder, 2021); Hartleb, Schliefsteiner and Schiebel, „From Anti-Measure to Anti-State"; Florian Hartleb and Christoph Schiebel, „Reichsbürger and Querdenken. Reacting to a growing concern for security," *EICTP Vienna Research Papers on Transnational Terrorism and Counter-Terrorism*, no. 6 (2024): 23-32, https://eictp.eu/wp-content/uploads/2024/07/EICTP_Research_Vienna-Papers_VI.pdf#page=25.

[29] Leyla Dogruel and Jost, Pablo „Radical Mobilization in Times of Crisis: Use and Effects of Appeals and Populist Communication Features in Telegram Channels," *Social Media + Society* 9, no. 3 (2023): 1-12, https://doi.org/10.1177/20563051231186372; Schrimpf et al., "Aus dem Channel, auf die Straße!"

[30] For cross-milieu intentions of extremists to exploit the pandemic see, i.e., Francesco Fairnelli, "Conspiracy theories and right-wing extremism – Insights and recommendations for P/CVE", (Luxembourg: Publications Office of the European Union, 2021), https://home-affairs.ec.europa.eu/system/files/2021-04/ran_conspiracy_theories_and_right-wing_2021_en.pdf; Gary Ackermann and Hayley Peterson, "Terrorism and COVID-19: Actual and Potential Impacts," *Perspectives on Terrorism* 14, no. 3 (2020): 59-73, https://www.jstor.org/stable/27158151. For the example of Reichsbürger see, i.e., Jan Rathje, „Durch die Krise ins Reich. Postpandemische Entwicklungen von 'Reichsbürgern' und Souveränist:innen in Deutschland" (CeMAS: Berlin, 2023), https://cemas.io/publikationen/durch-die-krise-ins-reich/.

31 Heidi Schulze, Julian Hohner, Simon Greipl, Maximilian Girgnhuber, Isabell Desta and Diana Rieger: „Far-right conspiracy groups on fringe platforms: a longitudinal analysis of radicalization dynamics on Telegram," *Convergence: The International Journal of Research into New Media Technologies* 28, no. 4 (2022): 1103-1126, https://doi.org/10.1177/13548565221104977; Ludwig-Maximilians-Universität zu München (LMU), „Mainstreaming und Radikalisierung in sozialen Medien. Forschungsvorhaben Online-Radikalisierung" (Cologne: Federal Office for the Protection of the Consitution, 2022), https://www.verfassungsschutz.de/DE/verfassungsschutz/auftrag/zusammenarbeit-imin-und-ausland/zentrum-fuer-analyse-und-forschung-zaf/zentrum-fuer-analyse-und-forschung-zaf_node.html; Forschungsstelle BAG „Gegen Hass im Netz" (BAG), „Subscribe to Subversion! Crossmediale Techniken der Gemeinschaftsbildung in rechtsalternativen Kontexten," *Machine Against the Rage* 6 (2024), https://doi.org/10.58668/matr/06.2.

32 Benjamin Lee, "Radicalisation and Conspiracy Theories," in *Routledge Handbook of Conspiracy Theories*, ed. Michael Butter and Peter Knight (London/New York: Routledge, 2020), 344-356.

33 Alex Mackenzie and Christian Kaunert, „Germany: Still „Auf dem rechten Auge blind"? in A Research Agenda for Far-Right Violence and Extremism, ed. Rohan Gunaratna and Katalin Pethö-Kiss (Edward Elgar Publishing: Cheltenham, 2024): 111-130, https://doi.org/10.4337/9781802209624.00011.

34 Initially representative for this trend is the Global Peace Index. It highlights a rise in violent demonstrations and a polarising decline of political attitudes, which includes higher levels of critical views of "existing administrative structures." The score deteriorated for full democracies by 73 percent from 2012 to 2022. The COVID-19 pandemic was discussed as having driven the deterioration between 2019 and 2021 in Europe and North America by another 29 percent. With a smaller sample size of 18 Western European countries, the RTV Trend Report 2022 showcases a change in targeting of group-based right-wing terrorism and violence against governments. The statistics of the BKA replicate this observation for Germany: for 2022, the number of offences against the state rose by 47.29 percent in comparison to 2021. Moreover, the number of politically motivated crimes in connection to the pandemic increased by 50.03 percent and predominantly targeted the state, their representative personnel, institutions or symbols. In contrast to the RTV Trend Report, almost all offences (90.78 percent) were labelled "unassignable" on the traditional extremism scale. However, the phenomenon is described to materialise both offline and online. Following the end of the pandemic, anti-government sentiments remain prominent online. See, Institute for Economics & Peace, "Global Peace Index 2022: Measuring Peace in a Complex World," (Sydney: Institute for Economics & Peace, 2022), 34, https://www.visionofhumanity.org/wp-content/uploads/2022/06/GPI-2022-web.pdf; Jacob Aasland Ravndal, Charlotte Tandberg, Anders Ravik Jupskås and Madeleine Thorstensen, "RTV Trend Report 2022. Right-Wing Terrorism and Violence in Western Europe, 1990 – 2021," *C-REX Research Report*, no. 1 (2022): i-38, https://www.sv.uio.no/c-rex/english/publications/c-rex-reports/2022/rtv_trend_report_2022.pdf; BKA and BMI, "Politisch motivierte Kriminalität," 18; Bàrbara Molas, Anne Craanen, Sabrina Tripodi, Kacper Rekawek and Thomas Renard, "Anti-Government Threats and their Transnational Connections," (Den Haag: International Centre for Counter-Terrorism, 2024), 20, https://www.icct.nl/publication/anti-government-threats-and-their-transnational-connections.

35 Brace, Baele and Ging for example describe a rise in ideological cross-pollination online through ecosystem outlinking, coining the concept of "exolinking". See also Anne Craanen, host, The Tech Against Terrorism Podcast, season 3, episode 11, "The Challenge of Hybrid Threats Online,", Tech Against Terrorism, 2023, March 23, 2023, 23 min., 40 sec.,https://podcast.techagainstterrorism.org/1684819/episodes/12493220; Kyler Ong, "Ideological Convergence in the Extreme Right," *Counter Terrorist Trends and Analyses* 12, no. 5 (2020): 2, https://www.jstor.org/stable/26954256; Lewys Brace, Stephane J. Baele and Debbie Ging, "Where do 'mixed, unclear and unstable' ideologies come from? A data-driven answer centred on the incelosphere," Journal of Policing, Intelligence and Counter Terrorism 19, no. 2 (2024): 106, doi: 10.1080/18335330.2023.2226667.

36 While the latest available report of the BfV (2023) highlights a continued blending of all observation categories, quarterly monitorings of the digital far-right ecosystem point towards steady activity of Reichsbürger and Querdenken accounts, despite of the latter partially loosing traction between summer 2023 and spring 2024. See Bundesministerium des Inneren und für Heimat (BMI), "Verfassungsschutzbericht 2023," (Berlin: Federal Ministry of the Interior and Community Germany, 2024), https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/verfassungsschutzberichte/2024-06-18-verfassungsschutzbericht-2023.pdf?__blob=publicationFile&v=17; Forschungsstelle BAG "Gegen Hass im Netz" (BAG), "Sommer 2023: Die Neue Web-Ordnung der Demokratiefeinde," Machine Against the Rage 4 (2024), https://www.doi.org/10.58668/matr/04.1; Forschungsstelle BAG "Gegen Hass im Netz" (BAG), "Sommer 2024: Drei Wahlen und ein Terrorfall," Machine Against the Rage 7 (2024), https://www.doi.org/10.58668/matr/07.1.

37 Braddock and Bjørgo, „Anti-Government Extremism"; Molas et al., "Anti-Government Threats";. Julia Ebner, Harvey Whitehouse and Christoph Kavanagh, „The QAnon Security Threat: A Linguistic Fusion-Based Violence Risk Assessment," *Perspectives on Terrorism* 16, no. 6 (2022): 62-86,

https://www.jstor.org/stable/27185092; Verna Fiebig and Daniel Koehler: „Uncharted Territory: Towards and Evidence-Based Criminology of Sovereign Citizens Through a Systematic Literature Review,“ *Perspectives on Terrorism* 16, no. 6 (2022): 34-48, https://www.jstor.org/stable/27185090; Bethany Leap and Michael Becker, „The Not-So-Silent „Majority“: An Automated Content Analysis of Anti-Government Online Communities,“ *Perspectives on Terrorism* 17, no. 1 (2023): 103-122, https://www.jstor.org/stable/27209221.

38 For work on issue-driven AGE see: Lydia Khalil and Joshua Roose, "Anti-Government Extremism in Australia: Understanding the Australian Anti-Lockdown Freedom Movement as a Complex Social Movement," *Perspectives on Terrorism* 17, no. 1 (2023): 144-169, https://www.jstor.org/stable/27209223; Isabelle Frens, Jelle van der Buuren and Edwin Bakker, "Rallying Around Empty Signifiers: Understanding and Defining Anti-Government Protest in the Netherlands," *Perspectives on Terrorism* 17, no. 2 (2023): 60-73, https://www.jstor.org/stable/27255592. For a systematic literature review on Sovereign Citizens see, Fiebig and Koehler, "Uncharted Territory."

39 Jan Rathje, "Driven by Conspiracies: The Justification of Violence among "Reichsbürger" and Other Conspiracy-Ideological Sovereignists in Contemporary Germany," *Perspectives on Terrorism* 16, no. 6 (2022): 49-61, https://www.jstor.org/stable/27185091; Jelle van der Buuren, "Breaking (with) the System: Exodus as Resistance?," *Perspectives on Terrorism* 17, no. 1 (2023): 88-103, https://www.jstor.org/stable/27209220.

40 Hartleb, Schliefsteiner and Schiebel, „From Anti-Measure to Anti-State“.

41 Jackson, "Anti-Government Extremism“; Braddock and Bjørgo, „Anti-Government Extremism“; Khalil and Roose, "Anti-Government Extremism in Australia."

42 The expression seems to be a specific term of the German language. Fischer highlights that there is no direct equivalent in any other language. English ones like "enemy image" were products of direct translations of German-language articles, which, however, were met with very little recognition. Therefore, the German term is used. See Fabian Fischer, *Die konstruierte Gefahr. Feindbilder im politischen Extremismus* (Baden Baden: Nomos, 2018), 55.

43 Ibid.

44 Jurgen Willems and Marc Jegers, "Social Movement Structures in Relation to Goals and Forms of Action: An Exploratory Model," *Canadian Journal of Nonprofit and Social Economy Research* 3, no. 2 (2012): 67-81.

45 Stefan Kühl, „Zur Gruppenförmigkeit terroristischer Zusammenschlüsse,“ in *Terrorismusforschung. Interdisziplinäres Handbuch für Wissenschaft und die Praxis*, ed. Liane Rothenberger et al. (Baden-Baden: Nomos, 2022), 121-134.

46 Braddock and Bjørgo, „Anti-Government Extremism“; Molas et al., "Anti-Government Threats."

47 Jackson, "Anti-Government Extremism," 10.

48 Molas et al., "Anti-Government Threats"; Goertz, Querdenker.

49 Emma A. Renström, Hanna Bäck and Holly M. Knapton, "Exploring a pathway to radicalization: The effects of social exclusion and rejection sensitivity," *Group Processes & Intergroup Relations* 23, no. 8 (2020): 1128, https://doi.org/10.1177/1368430220917215.

50 Laura G. E. Smith, Leda Blackwood, and Emma F. Thomas, "The Need to Refocus on the Group as the Site of Radicalization," *Perspectives on Psychological Science* 15, no. 2 (2019): 327, https://doi.org/10.1177/1745691619885870.

51 See, for example, David Meyer, „Protest and Political Opportunities,“ *Annual Review of Sociology*, no. 30 (2004): 125-145, https://www.annualreviews.org/content/journals/10.1146/annurev.soc.30.012703.110545.

52 David Meiering, Aziz Dziri, Naika Foroutan, Simon Teune, Esther Lehnert and Marwan Abou Taam, "Brückennarrative - Verbindende Elemente in der Radikalisierung von Gruppen," *PRIF-Report* 7 (2018): 1-33, https://www.prif.org/fileadmin/HSFK/hsfk_publikationen/prif0718.pdf.

53 J. M. Berger, *Extremism* (Cambridge/London: The MIT Press, 2018); John Horgan, *The Psychology of Terrorism* (London/New York: Routledge, 2005); Clark McCauley and Sophia Moskalenko, *Friction: How radicalization happens to them and us* (Oxford: Oxford University Press, 2011).

54 McCauley and Moskalenko, Friction, 220.

[55] Hansen, Hendrik, “Verfassungsschutzrelevante Delegitimierung des Staates: Eine Analyse des neuen Phänomenbereichs aus Sicht der Extremismusforschung,” in *Jahrbuch für Extremismus- und Terrorismusforschung 2021/2022 (1),* ed. Hendrik Hansen and Armin Pfahl-Traughber (Brühl/Rheinland: Hochschule des Bundes für öffentliche Verwaltung, 2024), 34-69.

[56] Pöhlmann, Rechte Esoterik.

[57] Jackson, “Anti-Government Extremism.”

[58] Smith, Blackwood and Thomas, “The Need.”

[59] Generally, it has to be noted that AGE is a „murky“ concept that comes with a lot of heuristic challenges. Jackson argues that AGE is a sub-category of right-wing extremism in the United States but this caterogisation may not be applicable for other countries or contexts. See Jackson, “Anti-Government Extremism.”

[60] QUERDENKEN-711, “Unser Manifest,” Querdenken-711, last accessed March 8, 2024, https://querdenken-711.de/manifest/.

[61] Pöhlmann, Rechte Esoterik.

[62] Jan-Gerrit Keil, “Zur Abgrenzung des Milieus der ‚Reichsbürger‘ – Pathologisierung des Politischen und Politisierung des Pathologischen,” Forensische Psychiatrie, Psychologie, Krimonologie, no. 15 (2021), https://doi.org/10.1007/s11757-021-00668-7.

[63] Hartleb, Schliefsteiner and Schiebel, “From Anti-Measure to Anti-State.”

[64] Paula Matlach and Dominik Hammer, “The German Far Right Online. A Longitudinal Study,” (London/Berlin: Institute for Strategic Dialogue, 2024, https://www.isdglobal.org/isd-publications/the-german-far-right-online-a-longitudinal-study/; Samantha Walther, and Andrew McCoy, “ US Extremism on Telegram: Fueling Disinformation, Conspiracy Theories, and Accelerationism,” *Perspectives on Terrorism* 15, no. 2 (2021): 100-124, https://www.jstor.org/stable/27007298; Jakob Guhl, Julia Ebner and Jan Rau, “The Online Ecosystem of the German Far-Right” (London: Institute for Strategic Dialogue, 2020), https://www.isdglobal.org/wp-content/uploads/2020/02/ISD-The-Online-Ecosystem-of-the-German-Far-Right-English-Draft-11.pdf.

[65] Matlach and Hammer, “The German Far Right Online”; Walther and McCoy, “US Extremism on Telegram”; Guhl et al., “Ecosystem of the German Far-Right”; Willems and Jegers, “Social Movement Structures.”

[66] Pablo Jost, Annett Heft, Kilian Buehling, Maximilian Zehring, Heidi Schulze, Hendrik Bitzmann and Emese Domahidi, “Mapping a Dark Space: Challenges in Sampling and Classifying Non-Instiutionalized Actors on Telegram,” *Medien & Kommunikationswissenschaft* 71, no. 3-4 (2023): 212-229, https://doi.org/10.5771/1615-634X-2023-3-4-2D12O.

[67] Kilian Buehling and Annett Heft, “Pandemic Protestors on Telegram: How Platform Affordances and Information Ecosystems Shape Digital Counterpublics,” *Social Media + Society* 9, no. 3 (2023): 1-19, https://doi.org/10.1177/20563051231199430.

[68] Silva Semenzin and Lucia Bainotti, “Dark Telegram,” Digital Methods Initiative, accessed July 6, 2023, https://wiki.digitalmethods.net/Dmi/SummerSchool2019DarkTelegram.

[69] Maximilian Zehring and Emese Domahidi, “German Protest Mobilizers on Telegram and Their Relations to the Far Right: A Network and Topic Analysis,” *Social Media + Society* 9, no. 1 (2023): 1-12, https://doi.org/10.1177/20563051231155106; Rathje, “Durch die Krise ins Reich.”

[70] Semenzin and Bainotti, “Dark Telegram.”

[71] Ibid.

[72] Stijn Peeters and Tom Willaert, “Telegram and Digital Methods: Mapping Networked Conspiracy Theories through Platform Affordances,” *M/C Journal* 25, no. 1 (2022): 3, https://doi.org/10.5204/mcj.2878.

[73] Stijn Peeters and Sal Hagen, “4CAT Capture and Analysis Toolkit: A Modular Tool for Transparent and Traceable Research,” *Computational Communication Research* 4, no. 2 (2022): 571-589, https://dx.doi.org/10.2139/ssrn.3914892.

[74] LMU, „Mainstreaming und Radikalisierung in sozialen Medien.“

[75] Schulze et al., „Far-Right Conspiracy Groups on Fringe Platforms“; LMU, „Mainstreaming und Radikalisierung in sozialen Medien.“

76 Cass R. Sunstein, "The Law of Group Polarization," *John M. Olin Program in Law & Economics Working Paper,* no. 91, (1999): 1-30, https://dx.doi.org/10.2139/ssrn.199668.

77 LMU, „Mainstreaming und Radikalisierung in sozialen Medien."

78 Both events stipulated shared radical actions of actors of Querdenken and Reichsbürger individuals. The flood in Ahrtal was especially instrumentalized by both milieus to criticize the (in-)action of the German government and mobilise within and outside of their communities under the disguise of helping the flood victims. See BMI, "Verfassungsschutzbericht 2021."

79 Ronny Junghans, "Vereinte Patrioten: Planungen konkreter als bisher gedacht," *Belltower News*, January 9, 2024, https://www.belltower.news/vereinte-patrioten-planungen-konkreter-als-bisher-gedacht-154951/.

80 Joachim Dankbar, "Fall 'Prinz Reuß': Todesliste aus Oberfranken," *Frankenpost*, December 12, 2023, https://www.frankenpost.de/inhalt.fall-prinz-reuss-hinrichtungslisten-aus-oberfranken.6a5507d4-cb8e-4f58-a871-80094146089e.html.

81 Schrimpf et al., "Aus dem Channel, auf die Straße!"

82 Molas et al., "Anti-Government Threats."

83 Georg Schuppener, *Restoring the Reich. The Language of the Reichsbürger* (Göttingen: V&R unipress, 2025).

84 Querdenken 711 – Stuttgart, "Unser Manifest," n.d., https://querdenken-711.de/manifest/.

85 Holzer et al., "Einleitung: Protest"; Willems and Jegers, "Social Movement Structure."

86 Jackson, "Anti-Government Extremism."

87 Joe Whittaker, "Rethinking Online Radicalization," *Perspectives on Terrorism* 16, no. 4 (2022): 27-40, https://www.jstor.org/stable/27158150.

88 Molas et al., "Anti-Government Threats."

89 Renström, Bäck and Knapton, "Exploring a pathway to radicalization," 1129.

90 BMI, "Verfassungsschutzbericht 2023," 145, 133.

PT PERSPECTIVES ON TERRORISM

Research Note

# In the Trenches: A Hands-on Pedagogical Approach to Teaching Data Collection Skills in Terrorism Studies

Sarah L. Carthy* and Yannick Veilleux-Lepage

Volume XIX, Issue 1
March 2025

ISSN: 2334-3745
DOI: 10.19165/2025.6984

**Abstract:** The burgeoning availability of open-source information on individuals who have been radicalised offers new opportunities to build, expand, and disaggregate rich databases on the characteristics of the phenomenon. However, this type of open-source data collection can be challenging to execute reliably, particularly when research teams include coders of varying skill levels. As the study of terrorism in higher education becomes increasingly formalised, the authors describe a scaffolded pedagogical approach to teaching and assessing the skill of data collection, one which formally integrated database creation into a master's level course on the topic of terrorism. As the authors reflect on field-wide challenges, including conceptual ambiguities which can prompt unreliable coding, methods for assessing acquired skills and competencies are also examined. In this way, it is hoped that this research note will contribute to efforts to advance the next generation of terrorism scholars, as well as support other educators seeking to incorporate authentic learning experiences into higher education courses.

**Keywords:** Far-right, radicalisation, military, data collection, reliability, teaching and learning

* *Corresponding author: Sarah L. Carthy, ISGA, Leiden University. Email: s.l.carthy@fgga.leidenuniv.nl*

# Introduction

The study of violence perpetrated by extremists, including terrorism, has always been informed by many disciplines, including political science, criminology, history, sociology, and psychology. The multidisciplinary nature of terrorism studies requires innovative approaches to research and teaching, as well as an appreciation of legal constraints, ethical concerns, and data biases that make it challenging to produce meaningful research. This research note outlines an approach for teaching and assessing the skill of data collection within a course on terrorism studies, detailing both its theoretical and conceptual underpinnings as well as its practical implementation: a dataset created by students on radicalised service personnel.

The approach is similar in structure and format to efforts developed at the National Consortium for the Study of Terrorism and Responses to Terrorism (START) at the University of Maryland, the National Counterterrorism Innovation, Technology, and Education Centre (NCITE) at the University of Nebraska Omaha, the Centre for Terrorism and Security Studies (CTSS) at the University of Massachusetts Lowell, and several other institutions of higher education, where students enrolled in terrorism studies courses and internships can become involved in hands-on collection and analysis of original data. These teams have produced several, widely respected databases on radicalised individuals and incidents of terrorism and, for this reason, our objective was not, necessarily, to replicate these efforts or outline how such a pursuit should be undertaken. Instead, our objective was pedagogical: to develop a scaffolded approach to conducting this type of data collection, one which would expose students to challenging coding decisions, for the first time, in a formal education setting.

As described in this research note, open-source data collection is often undertaken by research teams of varying levels of expertise and it is not uncommon for novice researchers to come face-to-face with challenging coding decisions, for the first time, in the field. Our approach sought to .equip students with the skills to navigate ethical dilemmas, such as respecting privacy while using open-source data, practical challenges, like verifying the reliability of sources, and methodological hurdles, including maintaining coding consistency across diverse data types. Throughout, we aimed to address the elusive and complex nature of data collection on the phenomenon of radicalisation, while also preparing students for the real-world challenges of countering it.

Against the backdrop of growing far-right radicalisation in various militaries around the world, master's degree students at Leiden University were provided with a list of names of individuals ('cases') with military or paramilitary backgrounds and links to far-right extremist groups or movements. Using a standardised codebook, these students coded each case using publicly available information, including court transcripts, journalistic accounts, and police reports. They navigated challenges such as contradictory reports from different media sources, missing legal documentation, and ambiguous terminology that made it difficult to classify certain behaviours accurately. This hands-on approach simulated real-world data collection contexts, immersing students in an authentic learning environment that refined their skills in handling raw, multilingual data from various sources. In addition, students deepened their understanding of racialisation trends and patterns.

# Gathering Data on Radicalised People

Acquiring high quality, representative data on radicalised people (including the relatively few who go on to become violent extremists or terrorists) can be challenging. Compared to other types of risky or extreme behaviour such as homicide or road-traffic accidents, the actual incidence of terrorist attacks is relatively low,[1] and those convicted under terrorist legislation are predominantly convicted of offenses that fall short of physical perpetration (e.g. weapons violations).[2] While those who undergo a process of radicalisation but do *not* act violently on their beliefs are certainly more prevalent in the general population than violent extremists,[3] these individuals rarely attract the attention of authorities, making them difficult to study.[4] As such, data on the arrest and prosecution of those suspected of involvement may only represent a subset of those who are truly radicalised.[5] This is especially the case for those who fear societal or professional reprisal for publicly voicing their extremist beliefs.

The quality of available data is an additional challenge. Even with ample data to draw upon, existing databases on radicalised individuals can be prone to sampling and selection biases,[6] and the sources used to provide information on radicalised individuals, ranging from legal documents to social media posts, may be inaccurate or biased. Media reports can be affected by location bias, national newspapers may not cover smaller, regional events, or coverage may be constrained by the amount of available space.[7] Indeed, even the political landscape at the time may influence how coders approach categorising certain behaviours or belief systems.[8] The quality of data is often further impeded by conceptual ambiguities, particularly for key terms like 'terrorism', 'extremism', and 'radicalisation' (an extensive body of literature details these debates elsewhere[9]). However, despite these challenges, several valuable coding instruments have been developed to capture the breadth and scope of data on radicalisation.

The most prominent codebook of its kind, compiled by the START consortium for the *Profiles of Individual Radicalisation in the United States* (PIRUS) database, captures details of the radicalisation trajectory such as whether the individual became involved in a plot, their affiliation with a violent extremist group, their criminal history, and biographical information relating to childhood, education, employment, and health. Here, the data tends to be gathered in teams. For example, the START consortium's PIRUS dataset,[10] the *American Terrorism Study* (ATS),[11] and the *Extremist Crime Database* (ECDB),[12] all utilise several coders to compile open-source information on cases and make coding decisions. While not without its limitations, this approach to data collection can expedite the data collection phase of a project in several ways. First, collecting data as part of a group allows for greater group deliberation, encouraging the coders to create a consistent, more informed coding logic. Second, on a more practical level, more skills and competencies are leveraged when there are several coders, including language skills. However, while it is certainly feasible to make reliable coding decisions in this way, inconsistency can be exacerbated by several factors, such as the dichotomous nature of the variables we include in our codebooks (this has notably been the case with the coding of 'mental disorder' and related constructs[13]), and the varying skill levels of coders.[14] When we look to other disciplines gathering biographical or behavioural data, for instance, novice coders tend to "index", rather than explicitly code.[15] Amidst these field-wide limitations, not only must students be trained to understand and, at times, conduct analyses on these types of data, but they must become familiar with the process of collecting it.

## Teaching Terrorism Studies in Higher Education

While contributing to ongoing data gathering projects in addition to one's studies certainly presents a unique learning opportunity for students, the argument for a formal, data collection course on radicalisation emerged, in part, from observing other disciplines using coding teams to gather behavioural data. In the health sciences, for instance, having teams comprised of different skill levels is not uncommon.[16] However, because training novice researchers tends to be resource heavy and, often, not feasible within the lifespan of a project,[17] the methodological training required to contribute to these projects tends to be more formalised.[18]

The impetus to create a course dedicated to collecting data on radicalised individuals was also borne, in part, out of structural considerations in the Dutch higher education context. In 2018, the Institute of Security and Global Affairs began offering this master's programme which was dedicated to crises arising from war, violence, cyber threats, natural disasters and, notably, terrorism. By incorporating active learning methods and enquiry-based learning, the programme prepares students to become reflective, academically trained crisis and security professionals. Upon enrolment in the programme, students choose to focus on one of six specialisations: *Governance of Violence*, *Governance of Crisis*, *Terrorism and Political Violence*,[19] *Cybersecurity and Governance*, *War and Peace Studies*, and *Intelligence and National Security*. To ensure the quality of teaching and assessment, the programme ceased offering a formal thesis assessment in 2020 and, instead, was restructured around four modules in which substantive knowledge, professional skills, and research skills were more seamlessly integrated to prepare students to work in a range of public, private, and civic sectors. In each block, students acquire a separate research skill: either literature reviewing, data collection, data analysis, or critical reflection. This means that course coordinators for each specialisation are tasked with creating a course in which a core research skill can be effectively honed within their area of study without a formal thesis assessment.

As course coordinators on the *Terrorism and Political Violence* track, our task was to integrate the skill of data collection into our course *Social Movements and Political Violence.*[20] To do so, we drew on our expertise in psychology and international relations respectively to develop a novel method of teaching and assessing data collection skills using open-source data.

## The 'Radicalised Service Personnel' Database

The infiltration of Western armed forces by radicalised individuals has been a longstanding national security concern. A widely held perception is that these 'radicalised soldiers', possessing specialist military skills (including proficiency in weapons and explosives), may use these skills to orchestrate devastating terrorist attacks.[21] Numerous law enforcement agencies have also cautioned that extremist factions are intentionally recruiting soldiers, not only to acquire access to weaponry and supplies, but also to recruit individuals with combat and medical expertise.[22] Despite the important nature of this phenomenon, few studies have examined the mechanisms underpinning the radicalisation of service members[23] and most inquiries on the subject rely on small, country-specific samples.[24] The *Radicalised Service Personnel* database was developed, in part, to address this oversight.

In advance of each academic year, we enlisted the support of a research assistant (usually a student from an earlier cohort) and compiled a list of names of individuals from Europe, the United Kingdom, or North America (including Canada) with military backgrounds who had come to the attention of authorities for activities related to the far-right. We created a list of cases that met the following inclusion criteria: individuals must have undergone at least basic military training, including roles as reservists, national guards, ROTC/ROTP, or coast guard members, prior to ceasing active involvement (Criterion 1). They must *also* demonstrate adherence to far-right ideologies through behavioural indicators such as online activities, attendance at far-right events or participation in acts of violent extremism (Criterion 2). Furthermore, their activities on behalf of the far-right movement must meet at least *one* of the following criteria: being arrested (or charged), indicted, or killed in action due to ideological activities; membership in a designated terrorist organisation, or; association with a violent extremist group with ideologically motivated indictments (Criterion 3). The names of radicalised individuals were identified through reviews of scholarly literature, government and non-government reports, and Google alerts based on specific keywords. The list of cases was updated throughout the year, with new cases added as new information became available from government reports, news articles, and research publications. This "evergreen" process ensured that each cohort in September worked with the most up-to-date list of radicalised service personnel.

Each year, students were provided with the list of cases that had been assigned to their cohort along with a codebook which contained a list of variables, usually categorical in nature, to be coded by the class. To re-create the environment in which this type of data collection typically unfolds, the 40-item codebook was modified from the PIRUS codebook, as well as the Schuurman and Carthy's *Non-Involved in Terrorist Violence* (NITV) codebook.[25] As a pedagogical tool, it was necessary that the codebook was an appropriate length (half the size of established ones) and contained clear, unambiguous variables which students could code without much difficulty (e.g., year of birth or marital status) as well as more complicated variables which required them to consider their rationale more extensively. This is because, as mentioned, this type of data collection is susceptible to bias, and it is important that students understand how coding decisions are made, including poor ones.

Variables such as whether an individual could be categorised as having participated in violence, for instance, can vary coder to coder. Some may consider those who have been legally charged with having "engaged in terrorist activity"[26] as having participated in violence. Others, however, may consider "engagement" to be a much broader category of behaviour. Someone who is charged with engagement in terrorist activities may have had "intent" or "capability" but ultimately not succeeded.[27] Engagement may also represent the *process* by which an individual comes to identify with a terrorist cause, rather than the violent act itself. Due to these ambiguities, such variables often prompt inconsistent coding decisions and would be considered, by most radicalisation scholars, *unreliable* coding instruments. This underscores the pedagogical nature of this exercise. We introduced these "sticky" variables, such as the definition of 'engagement in terrorism,' to push students to critically evaluate evidence and consider the nuances of interpretation. These variables required students to apply logic and engage in group deliberation, fostering skills in collaborative decision-making and addressing the inherent ambiguities in real-world data. In fact, it was these elements, independent research, and group deliberation, which formed a paradigmatic element of the approach more broadly.

## A Scaffolded Approach

It is important to emphasise that students on the master enter the course with diverse backgrounds in terms of research skills. While the majority come from the social sciences and have some experience collecting and analysing data on social phenomena, others are less familiar with this type of research, have never worked with larger datasets and/or are unfamiliar with Microsoft Excel.[28] As educators, we knew it was important to offer students the opportunity to hone their data collection skill individuall*y* before working together in a group. For this reason, we took a scaffolded approach, assigning students a smaller assignment at the beginning of the course so that they could learn how to use a codebook and gather supporting evidence before gathering data as part of a group.

This individual assignment varied year-to-year, but in its earliest iterations, students were required to identify at least twenty vehicle ramming attacks against Black Lives Matter (BLM) protests or protesters in the United States within a specific three-month period. Vehicle ramming attacks against BLM members were chosen because the nature of the events is relatively unambiguous, and the use of vehicle ramming attacks represented a new addition within the tactical repertoire of the far-right in the United States.[29] Using a codebook of four items, students were required to gather evidence to justify the inclusion of these attacks in their dataset (determining whether the vehicle was the primary weapon in the attack, whether it was used against civilians, whether it took place in the scope of BLM and, finally, whether it was rooted in a desire for political, economic, religious, or social change). Students who performed poorly on this assignment tended to use untrustworthy sources (e.g., tabloids), not enough sources (e.g., a singular source or circular reporting) or failed to demonstrate how the cited source supported their coding decision (e.g., failing to include direct quotations or having excessively long quotations). Some students admitted to feeling "overwhelmed" by their first encounter with data collection, others did not see the value in having such "similar" data collection assignments. Nonetheless, by having students conduct this type of research independently (and receive individual feedback), we sought to ensure that each student could contribute to a larger, data collection exercise in a more authentic setting: as part of a team.

As discussed in earlier sections, data of this nature are typically collected by teams of researchers and research assistants. At the beginning of the course, we asked students to complete a short questionnaire indicating their language competencies, and this allowed us to create multilingual groups of eight to ten students. All groups contained several Dutch speakers and at least two or three who spoke German, French, or Spanish. All group members spoke English and many also spoke non-European languages such as Arabic, Hebrew, and Mandarin. With individual feedback on their data collection skills, a multilingual group, a fresh list of fifty radicalised military personnel as well as a detailed codebook, the groups were ready to start data collection.

## The Messy World of Data Collection

Students had three weeks to complete the assignment and would typically allocate different cases to different group members. Often, one group member would be allocated one or two fewer cases and would, in turn, bear responsibility for populating the Excel spreadsheet using the correct style guidelines prior to submission. Lectures continued throughout this period and, as instructors, we found ways to connect course content to students' mutual experience of collecting data. We spoke, for instance, about the limitations of open-source data collection, as well as its potential to create a more extensive, descriptive understanding of radicalisation.

As a strategy for deeper collaboration, we would set aside time at the beginning of each lecture for students to ask questions about the assignment. They would often speak about cases they were struggling with, or request clarity on certain variables. This time allowed students to exchange ideas and sharpen their logic, often with us, as instructors, taking a step back to allow students to engage in active learning. They learned how other students may approach certain variables differently, perhaps because of their undergraduate training or even personal backgrounds. There was a great deal of debate, for instance, about how to code cases who were involved in the storming of the US Capitol. Ten percent of those who breached the perimeter of the US Capitol Building on 6 January 2021 were military veterans,[30] but not all participated in the same way. Should all Capitol cases be coded as radicalised or involved in a violent plot, or should they be coded based on the particularity of their individual actions during the event? Here, students would learn that it was more important that they were consistent with their *own group's* coding, rather than striving for uniformity with *other groups'* coding. This allowed students to relax into the assignment and learn that 'right' or 'wrong' answers didn't always exist.

Developing the *Radicalised Service Personnel* dataset can easily be described as a tedious undertaking. Not only is this type of research time-consuming, but the application of the codebook to open-source data can breed frustration and it is important that students learn why this is the case. As alluded to in earlier sections, the empirical study of radicalisation is a burgeoning field and, as such, the operationalisation of central concepts continues to be disputed. Furthermore, the field is theoretically underdeveloped, meaning that theoretical frameworks informing key processes tend to have poor explanatory power.[31] It is, therefore, unsurprising that the variables which trickle down into our codebook, such as whether an individual 'joined' an extremist group or could be considered 'involved' in a violent plot, also suffer shortcomings. In class, students would ask questions about particular variables or cases and become exasperated at the "ambiguous" nature of the codebook, or the elusiveness of the cases assigned to them. This was important as we wanted students to overcome these challenges and determine, namely, when it was appropriate to not code a particular variable. In assessing whether students had acquired the data collection skill, we determined whether there was evidence of ill-informed coding (i.e., filling out an item in the codebook, despite not having enough high-quality sources to support the observation) or lazy coding (i.e., marking an item as 'unknown' when high quality sources to support the observation did exist) and these instances culminated in an overall points reduction.

As a mechanism to prevent free-riding, students also completed an evaluation of each team member after the assignment was submitted. Each team member was scored out of ten for the quality and quantity of their contribution, their level of professionalism and communication. There was also an open-ended section where they could reflect on the dynamics within the group. When the assignment was graded, this evaluation accounted for 30 percent of the overall grade for the data collection assignment.

## Conclusion

For decades now, the study of radicalisation has welcomed innovative methodologies from a range of academic disciplines. As the nature and quality of the data we gather changes and develops, it is imperative that students of terrorism studies learn to become critical consumers of these data before entering the field. The objective of the approach described here was not necessarily distinguished by the creation of a new dataset of radicalised individuals but, instead, by its pedagogical goals. Against the backdrop of growing far-right radicalisation amongst service personnel in Europe, the United States and Canada, students learned how to access open-source data, apply a codebook, make coding decisions and work as part of a team to input data into the first dataset of its kind. In this way, we sought to immerse students in an authentic, data collection environment, one which represented the field as it is today; rich and messy. The exercise presented novel learning opportunities for students, such as how to operationalise different manifestations of radicalisation, when to 'dig deeper' and, importantly, when to simply 'give up' on a case. Indeed, one of the key learning objectives of this approach was for students to better understand the limitations of this type of research. These learning experiences, particularly the use of real-life data, also allowed students to develop expertise in the growing phenomenon of extremism within Western militaries, which they could then leverage after graduation. Several students have engaged in both paid and unpaid research assistantships on this topic, and at least one has co-authored two pieces on the topic of extremism within the military, contributing valuable insights to the field.[32]

As the study of terrorism increasingly relies on quantitative methodologies, we hope the pedagogical approach described here encourages other instructors in the field to recognise the possibilities of these data to train the next generation of scholars. By engaging in this type of hands-on learning, students may be better prepared to contribute meaningfully to the evolving field of terrorism studies, bringing both critical analysis and practical skills to bear on complex global issues.

*Sarah L. Carthy is an assistant professor of terrorism and political violence at the Institute of Security and Global Affairs at Leiden University in the Netherlands. She is a graduate of the University of Galway where she completed her BA and PhD in Psychology.*

*Yannick Veilleux-Lepage is an assistant professor in the Department of Political Science and Economics at the Royal Military College of Canada. Previously, he served as an assistant professor of terrorism and political violence at Leiden University's Institute of Security and Global Affairs.*

*Acknowledgements: We would like to thank each cohort of students who have taken our course over the years. Your hard work, enthusiasm and feedback have been invaluable.*

# Endnotes

[1] Stephen C. Nemeth and Jacob A. Mauslein, ‘Location Matters: Average Annual Risk of Domestic Terrorism, 1990-2010–A Subnational Analysis’, *Journal of Regional Security* 14, no. 1 (2019): 29–32; Charles L. Ruby, ‘The Definition of Terrorism’, *Analyses of Social Issues and Public Policy* 2, no. 1 (2002): 9–14.

[2] Monica Lloyd and Christopher Dean, ‘The Development of Structured Guidelines for Assessing Risk in Extremist Offenders.’, *Journal of Threat Assessment and Management* 2, no. 1 (2015): 52.

[3] Bart Schuurman, ‘Non-Involvement in Terrorist Violence’, *Perspectives on Terrorism* 14, no. 6 (2020): 14–26.

[4] Sarah L. Carthy and Bart Schuurman, ‘Researching Extremists and Terrorists: Reflections on Interviewing Hard-to-Reach Populations’, in *Fieldwork Experiences in Criminology and Security Studies: Methods, Ethics, and Emotions* (Springer, 2023), 375–98.

[5] Gary LaFree, Nancy A. Morris, and Laura Dugan, ‘Cross-National Patterns of Terrorism: Comparing Trajectories for Total, Attributed and Fatal Attacks, 1970–2006’, *The British Journal of Criminology* 50, no. 4 (2010): 622–49.

[6] Charles W. Mahoney, *More Data, New Problems: Audiences, Ahistoricity, and Selection Bias in Terrorism and Insurgency Research* (Oxford University Press, 2018); Deven Parekh et al., ‘Studying Jihadists on Social Media: A Critique of Data Collection Methodologies’, *Perspectives on Terrorism* 12, no. 3 (2018): 5–23.

[7] Yannick Veilleux-Lepage, *Terror Evolves: The Emergence and Spread of Terrorist Techniques* (Rowman & Littlefield, 2020)

[8] Bart Schuurman and Sarah L. Carthy, ‘The Makings of a Terrorist: Continuity and Change across Left-, Right-and Jihadist Extremists and Terrorists in Europe and North-America, 1960s-Present’, *Deviant Behavior*, 2022, 1–22.

[9] John M Berger, *Extremism* (Mit Press, 2018); Boaz Ganor, ‘Defining Terrorism: Is One Man’s Terrorist Another Man’s Freedom Fighter?’, *Police Practice and Research* 3, no. 4 (2002): 287–304; Arun Kundnani, ‘Radicalisation: The Journey of a Concept’, *Race & Class* 54, no. 2 (2012): 3–25.

[10] Note: Students were involved in developing the Profiles of Individual Radicalization in the United States (PIRUS) database at the National Consortium for the Study of Terrorism and Responses to Terrorism (START). The project has historically relied on research assistants, including graduate and undergraduate students, to help collect and code data under the supervision of senior researchers. These students typically work on gathering open-source information about individuals in the dataset, verifying details, and coding variables related to radicalisation pathways, demographics, and extremist affiliations. Their contributions play a role in ensuring the robustness and accuracy of the dataset. Students have also been involved in developing and maintaining the American Terrorism Study (ATS). The ATS, which was originally started by Brent Smith in the late 1980s, has relied on research assistants, including graduate and undergraduate students, to assist with data collection, case coding, and analysis. These students typically help review court records, law enforcement reports, and other public documents to code information about terrorist incidents, perpetrators, and group affiliations. Their contributions have been essential in expanding the dataset and ensuring its accuracy over time. And students have been involved in developing the Extremist Crime Database (ECDB). The project, which is maintained by researchers at various academic institutions, including those affiliated with the University of Maryland’s START centre, has relied on graduate and undergraduate research assistants to collect, verify, and code data. These students help analyse court records, news sources, and other open-source materials to track criminal activities associated with extremist individuals and groups in the United States. Their work has been essential in expanding the dataset and ensuring the reliability of the information.

[11] Brent L. Smith and Kelly R. Damphousse. ‘American Terrorism Study, 1980-2002’, *Inter-university Consortium for Political and Social Research* (2007).

[12] Joshua D. Freilich et al., ‘Introducing the United States Extremis Crime Database (ECDB)’, *Terrorism and Political Violence* 26, no. 2 (2014): 372–84.

[13] Kiran M. Sarma, Sarah L. Carthy, and Katie M. Cox, ‘Mental Disorder, Psychological Problems and Terrorist Behaviour: A Systematic Review and Meta-analysis’, *Campbell Systematic Reviews* 18, no. 3 (2022): e1268.

[14] Hruschka et al., ‘Reliability in Coding Open-Ended Data: Lessons Learned from HIV Behavioral Research’.

[15] Daniel J Hruschka et al., ‘Reliability in Coding Open-Ended Data: Lessons Learned from HIV Behavioral Research’, *Field Methods* 16, no. 3 (2004): 307–31.

[16] Wendy A Hall et al., ‘Qualitative Teamwork Issues and Strategies: Coordination through Mutual Adjustment’, *Qualitative Health Research* 15, no. 3 (2005): 394–410; Hruschka et al., ‘Reliability in Coding Open-Ended Data: Lessons Learned from HIV Behavioral Research’; M Ariel Cascio et al., ‘A Team-Based

Approach to Open Coding: Considerations for Creating Intercoder Consensus', *Field Methods* 31, no. 2 (2019): 116–30.

17 Wendy A Hall et al., 'Qualitative Teamwork Issues and Strategies: Coordination through Mutual Adjustment', *Qualitative Health Research* 15, no. 3 (2005): 394–410; Hruschka et al., 'Reliability in Coding Open-Ended Data: Lessons Learned from HIV Behavioral Research'; M Ariel Cascio et al., 'A Team-Based Approach to Open Coding: Considerations for Creating Intercoder Consensus', *Field Methods* 31, no. 2 (2019): 116–30.

18 Emily M D'Agostino, WayWay M Hlaing, and James H Stark, 'Teaching on the Continuum: Epidemiology Education From High School Through Graduate School', *Am J Epidemiol* 188, no. 6 (2019): 979–86.

19 Before 2025, this track was titled the *Governance of Radicalism, Extremism, and Terrorism* track.

20 Since 2025, the course has been re-titled *Extremist Thinking*.

21 Daniel Koehler, *A Threat from Within?: Exploring the Link Between the Extreme Right and the Military* (JSTOR, 2019); Teun Van Dongen et al., 'Right-Wing Extremism in the Military: A Typology of the Threat', *ICCT Research Papers*, 2022; Yannick Veilleux-Lepage and E Leidig, 'Investigating the Radical Right's Presence in the Canadian Military', *The Radical Right During Crisis: CARR Yearbook 2020/2021*, 2021, 202–6.

22 *The New York Times*, 'Extremists in Uniform Put the Nation at Risk', 13 November 2022, https://www.nytimes.com/2022/11/13/opinion/us-police-military-extremism.html; Travis Tritten et al., 'The Threat from Extremist Groups Is Growing. Service Members and Vets Are Getting Sucked into the Violence', *Military.Com*, 5 April 2023, https://www.military.com/daily-news/2023/04/05/threat-extremist-groups-growing-service-members-and-vets-are-getting-sucked-violence.html.

23 Håvard Haugstvedt and Daniel Koehler, 'Armed and Explosive? An Explorative Statistical Analysis of Extremist Radicalization Cases with Military Background', *Terrorism and Political Violence* 35, no. 3 (2023): 518–32; Klaus Roghmann and Wolfgang Sodeur, 'The Impact of Military Service on Authoritarian Attitudes: Evidence from West Germany', *American Journal of Sociology* 78, no. 2 (1972): 418–33.

24 Van Dongen et al., 'Right-Wing Extremism in the Military: A Typology of the Threat'.

25 Bart Schuurman and Sarah L Carthy, 'Understanding (Non) Involvement in Terrorist Violence: What Sets Extremists Who Use Terrorist Violence Apart from Those Who Do Not?', *Criminology & Public Policy*, 2023; Bart Schuurman and Sarah L Carthy, 'Who Commits Terrorism Alone? Comparing the Biographical Backgrounds and Radicalization Dynamics of Lone-Actor and Group-Based Terrorists', *Crime & Delinquency*, 2023, 00111287231180126; Bart Schuurman and Sarah L Carthy, 'Contextualizing Involvement in Terrorist Violence by Considering Non-Significant Findings: Using Null Results and Temporal Perspectives to Better Understand Radicalization Outcomes', *Plos One* 18, no. 11 (2023): e0292941.

26 Erin Miller and Kathleen Smarick, 'Profiles of Perpetrators of Terrorism in the United States: Research Highlight' (College Park, MD: START, 2012), https://www.start.umd.edu/pubs/START_ProfilesofPerpetratorsofTerrorismintheUS_ResearchHighlight_July2014.pdf.

27 Monica Lloyd and Christopher Dean, 'The Development of Structured Guidelines for Assessing Risk in Extremist Offenders.', *Journal of Threat Assessment and Management* 2, no. 1 (2015): 42.

28 While we debated using a more fit-for-purpose dataset management software such as NocoBD or Airtable, we settled on Excel due to its accessibility. Students at our university receive access to the Microsoft 365 product suite which is compatible with both Mac and Windows computers, and it was likely that knowledge of Excel would serve them well in the future.

29 Yannick Veilleux-Lepage, "The Radical Right Legitimisation of Vehicle Ramming," in *Tracking the Rise of the Radical Right Globally* (Ibidem-Verlag, 2019), 305-308; Amy-Louise Williams, Emily Corner, and Helen Taylor, 'Vehicular Ramming Attacks: Assessing the Effectiveness of Situational Crime Prevention Using Crime Script Analysis', *Terrorism and Political Violence* 34, no. 8 (2022): 1549–1563.

30 Eric B. Hodges, '"Storming the Castle."Examining the Motivations of the Veterans Who Participated in the Capitol Riots', *Journal of Veterans Studies* 7, no. 3 (2021): 46–59.

31 Sarah L Carthy and Bart Schuurman, 'Adverse Childhood Experiences, Education, and Involvement in Terrorist Violence: Examining Mediation and Moderation', *Journal of School Psychology* 106 (2024): 101348.

32 The experience of one graduate is illustrative. Her expertise in coding and analysing radicalisation data, honed during the course, enabled her to contribute to key research projects on military extremism, highlighting the value of hands-on learning in professional settings. She later co-authored two significant pieces on the topic of extremism within the military, contributing valuable insights to the field: Hanna Rigault Arkis and Jessica White, 'Female Veterans and Right-Wing Extremism: Becoming "One of

the Boys"', 28 January 2022, https://www.icct.nl/publication/female-veterans-and-right-wing-extremism-becoming-one-boys; Van Dongen et al., 'Right-Wing Extremism in the Military: A Typology of the Threat'.

## Bibliography

Berger, John M. *Extremism*. Mit Press, 2018.

Carthy, Sarah L, and Bart Schuurman. 'Adverse Childhood Experiences, Education, and Involvement in Terrorist Violence: Examining Mediation and Moderation'. *Journal of School Psychology* 106 (2024): 101348.

———. 'Researching Extremists and Terrorists: Reflections on Interviewing Hard-to-Reach Populations'. In *Fieldwork Experiences in Criminology and Security Studies: Methods, Ethics, and Emotions*, 375–98. Springer, 2023.

Cascio, M Ariel, Eunlye Lee, Nicole Vaudrin, and Darcy A Freedman. 'A Team-Based Approach to Open Coding: Considerations for Creating Intercoder Consensus'. *Field Methods* 31, no. 2 (2019): 116–30.

D'Agostino, Emily M, WayWay M Hlaing, and James H Stark. 'Teaching on the Continuum: Epidemiology Education From High School Through Graduate School'. *Am J Epidemiol* 188, no. 6 (2019): 979–86.

Freilich, Joshua D., Steven M. Chermak, Roberta Belli, Jeff Gruenewald, and William S. Parkin. 'Introducing the United States Extremis Crime Database (ECDB)'. *Terrorism and Political Violence* 26, no. 2 (2014): 372–84.

Ganor, Boaz. 'Defining Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter?' *Police Practice and Research* 3, no. 4 (2002): 287–304.

Hall, Wendy A, Bonita Long, Nicole Bermbach, Sharalyn Jordan, and Kathryn Patterson. 'Qualitative Teamwork Issues and Strategies: Coordination through Mutual Adjustment'. *Qualitative Health Research* 15, no. 3 (2005): 394–410.

Haugstvedt, Håvard, and Daniel Koehler. 'Armed and Explosive? An Explorative Statistical Analysis of Extremist Radicalization Cases with Military Background'. *Terrorism and Political Violence* 35, no. 3 (2023): 518–32.

Hodges, Eric B. '"Storming the Castle."Examining the Motivations of the Veterans Who Participated in the Capitol Riots'. *Journal of Veterans Studies* 7, no. 3 (2021): 46–59.

Hruschka, Daniel J, Deborah Schwartz, Daphne Cobb St. John, Erin Picone-Decaro, Richard A Jenkins, and James W Carey. 'Reliability in Coding Open-Ended Data: Lessons Learned from HIV Behavioral Research'. *Field Methods* 16, no. 3 (2004): 307–31.

Koehler, Daniel. *A Threat from Within?: Exploring the Link Between the Extreme Right and the Military*. JSTOR, 2019.

Kundnani, Arun. 'Radicalisation: The Journey of a Concept'. *Race & Class* 54, no. 2 (2012): 3–25.

LaFree, Gary, Nancy A. Morris, and Laura Dugan. 'Cross-National Patterns of Terrorism: Comparing Trajectories for Total, Attributed and Fatal Attacks, 1970–2006'. *The British Journal of Criminology* 50, no. 4 (2010): 622–49.

Lloyd, Monica, and Christopher Dean. 'The Development of Structured Guidelines for Assessing Risk in Extremist Offenders.' *Journal of Threat Assessment and Management* 2, no. 1 (2015): 40.

Mahoney, Charles W. *More Data, New Problems: Audiences, Ahistoricity, and Selection Bias in Terrorism and Insurgency Research*. Oxford University Press, 2018.

Miller, Erin, and Kathleen Smarick. 'Profiles of Perpetrators of Terrorism in the United States: Research Highlight'. College Park, MD: START, 2012. https://www.start.umd.edu/pubs/START_ProfilesofPerpetratorsofTerrorismintheUS_ResearchHighlight_July2014.pdf.

Nemeth, Stephen C., and Jacob A. Mauslein. 'Location Matters: Average Annual Risk of Domestic Terrorism, 1990-2010–A Subnational Analysis'. *Journal of Regional Security* 14, no. 1 (2019): 29–32.

Parekh, Deven, Amarnath Amarasingam, Lorne Dawson, and Derek Ruths. 'Studying Jihadists on Social Media: A Critique of Data Collection Methodologies'. *Perspectives on Terrorism* 12, no. 3 (2018): 5–23.

Rigault Arkis, Hanna, and Jessica White. 'Female Veterans and Right-Wing Extremism: Becoming "One of the Boys"', 28 January 2022. https://www.icct.nl/publication/female-veterans-and-right-wing-extremism-becoming-one-boys.

Roghmann, Klaus, and Wolfgang Sodeur. ‘The Impact of Military Service on Authoritarian Attitudes: Evidence from West Germany’. *American Journal of Sociology* 78, no. 2 (1972): 418–33.

Ruby, Charles L. ‘The Definition of Terrorism’. *Analyses of Social Issues and Public Policy* 2, no. 1 (2002): 9–14.

Sarma, Kiran M., Sarah L. Carthy, and Katie M. Cox. ‘Mental Disorder, Psychological Problems and Terrorist Behaviour: A Systematic Review and Meta-analysis’. *Campbell Systematic Reviews* 18, no. 3 (2022): e1268.

Schuurman, Bart. ‘Non-Involvement in Terrorist Violence’. *Perspectives on Terrorism* 14, no. 6 (2020): 14–26.

Schuurman, Bart, and Sarah L Carthy. ‘Contextualizing Involvement in Terrorist Violence by Considering Non-Significant Findings: Using Null Results and Temporal Perspectives to Better Understand Radicalization Outcomes’. *Plos One* 18, no. 11 (2023): e0292941.

Schuurman, Bart, and Sarah L. Carthy. ‘The Makings of a Terrorist: Continuity and Change across Left-, Right-and Jihadist Extremists and Terrorists in Europe and North-America, 1960s-Present’. *Deviant Behavior*, 2022, 1–22.

Schuurman, Bart, and Sarah L Carthy. ‘Understanding (Non) Involvement in Terrorist Violence: What Sets Extremists Who Use Terrorist Violence Apart from Those Who Do Not?’ *Criminology & Public Policy*, 2023.

———. ‘Who Commits Terrorism Alone? Comparing the Biographical Backgrounds and Radicalization Dynamics of Lone-Actor and Group-Based Terrorists’. *Crime & Delinquency*, 2023, 00111287231180126.

The New York Times. ‘Extremists in Uniform Put the Nation at Risk’, 13 November 2022. https://www.nytimes.com/2022/11/13/opinion/us-police-military-extremism.html.

Tritten, Travis, Drew Lawrence, Konstantin Toropin, and Steve Beynon. ‘The Threat from Extremist Groups Is Growing. Service Members and Vets Are Getting Sucked into the Violence’. *Military.Com*, 5 April 2023. https://www.military.com/daily-news/2023/04/05/threat-extremist-groups-growing-service-members-and-vets-are-getting-sucked-violence.html.

Van Dongen, Teun, YD Veilleux-Lepage, Eviane Leidig, and H Rigault Arkis. ‘Right-Wing Extremism in the Military: A Typology of the Threat’. *ICCT Research Papers*, 2022.

Veilleux-Lepage, Yannick, and E Leidig. ‘Investigating the Radical Right’s Presence in the Canadian Military’. *The Radical Right During Crisis: CARR Yearbook 2020/2021*, 2021, 202–6.

PERSPECTIVES ON TERRORISM

BIBLIOGRAPHY

# Bibliography: Critical Infrastructure Security – Prevention, Preparedness, and Response to Terrorist Attacks

Judith Tinnes*

Volume XIX, Issue 1
March 2025

ISSN: 2334-3745

**Abstract:** This bibliography contains journal articles, book chapters, books, edited volumes, theses, grey literature, bibliographies and other resources on critical infrastructure security. It focuses on the prevention, preparedness, and response to terrorist and insurgent attacks. The bibliography prioritises recent publications (up to January 2025) and should not be considered as being exhaustive. The literature has been retrieved by manually browsing more than 200 core and periphery sources in the field of Terrorism Studies. Additionally, full-text as well as reference retrieval systems have been employed to broaden the search.

**Keywords:** Bibliography, resources, literature, critical infrastructure security, critical infrastructure protection, terrorism, prevention, preparedness, response, resiliency, emergency management, crisis communication

*NB: All websites were last visited on 02.02.2025. For an inventory of previous bibliographies, see: https://archive.org/details/terrorism-research-bibliographies*

* *Corresponding author: Judith Tinnes, Terrorism Research Initiative, email: j.tinnes@gmx.de*

## Bibliographies and other Resources

Aviation Safety Network (ASN) (1996, January-): *ASN Aviation Safety Database*. URL: https://aviation-safety.net/database

Critical Infrastructures Preparedness and Resilience Research Network (CIPRNet) (2013, March-): URL: https://ciprnet.eu

McDonald, Brody (2021, February): Preparedness for, and Resilience to, Terrorism: Bibliography 60+ Full-Text Academic Theses (Ph.D. and M.A.) Written in English Between 2000 and 2020. Perspectives on Terrorism, 15(1), 228-232. URL: https://www.jstor.org/stable/26984811

Nelson, Christopher et al. (2024, March): *Incident Management Measurement Toolkit*. (RAND Tools, TL-A3196-1). DOI: https://doi.org/10.7249/TLA3196-1

Ramsay, James (Ed.-in-Chief) (2004, January-): *Journal of Homeland Security and Emergency Management*. [ISSN: 1547-7355]. URL: https://www.degruyter.com/journal/key/jhsem/html

Scrivens, Ryan (2019, February): 475 Academic Theses (Ph.D. and MA) on Countering Violent Extremism (CVE), Preventing Violent Extremism (PVE) and Terrorism Prevention (Written in Dutch, English, French, German, Italian, Norwegian, and Spanish). *Perspectives on Terrorism*, 13(1), 197-228. URL: https://www.jstor.org/stable/26590531

Shapiro, Lauren R.; Maras, Marie-Helen (Eds.) (2020): *Encyclopedia of Security and Emergency Management*. [Living Reference Work]. Cham: Springer. DOI: https://doi.org/10.1007/978-3-319-69891-5

Singh, Ishaansh (2021): General Bibliography on Terrorism Prevention and Preparedness. In: Alex P. Schmid (Ed.): *Handbook of Terrorism Prevention and Preparedness*. The Hague: ICCT Press, 1159-1259. URL: https://www.icct.nl/publication/handbook-terrorism-prevention-and-preparedness

Thomas, Andrew R. (Ed.-in-Chief) (2008, March-): *Journal of Transportation Security*. [p-ISSN: 1938-7741; e-ISSN: 1938-775X]. URL: https://link.springer.com/journal/12198

Tinnes, Judith (2019, December): Bibliography: Terrorism Prevention. *Perspectives on Terrorism,* 13(6), 116-166. URL: https://www.jstor.org/stable/26853765

Tinnes, Judith (2024, March): Bibliography: Risk Assessment of Terrorism. *Perspectives on Terrorism*, 18(1), 144-207. URL: https://pt.icct.nl/sites/default/files/2024-03/Bibliography_final%20version_0.pdf

Transportation Security Administration (TSA) (n.d.): *Transportation Security Timeline*. URL: https://www.tsa.gov/timeline

## Books and Edited Volumes

Abbas, Ali E.; Tambe, Milind; von Winterfeldt, Detlof (Eds.) (2017): *Improving Homeland Security Decisions*. New York: Cambridge University Press. DOI: https://doi.org/10.1017/9781316676714

Alperen, Martin J. (Ed.) (2017): *Foundations of Homeland Security: Law and Policy*. (2nd ed.). (Wiley Series on Homeland Defense and Security). Hoboken: John Wiley & Sons.

Apostol, Ion et al. (2015): *Engaging the Public to Fight the Consequences of Terrorism and Disasters*. (NATO Science for Peace and Security Series – E: Human and Societal Dynamics, Vol. 120). Amsterdam: IOS Press.

Atlas, Randall I. (2013): *21st Century Security and CPTED: Designing for Critical Infrastructure Protection and Crime Prevention*. (2nd ed.). Boca Raton: CRC Press. DOI: https://doi.org/10.1201/b15046

Baggett, Ryan K.; Simpkins, Brian K. (2018): *Homeland Security and Critical Infrastructure Protection*. (2nd ed.). (Praeger Security International). Santa Barbara: Praeger.

Balomenos, Konstantinos P.; Fytopoulos, Antonios; Pardalos, Panos M. (Eds.) (2023): *Handbook for Management of Threats: Security and Defense, Resilience and Optimal Strategies.* (Springer Optimization and Its Applications, Vol. 205). Cham: Springer. DOI: https://doi.org/10.1007/978-3-031-39542-0

Barnosky, Jason Thomas et al. (2024, March): *Improving Assessments in Emergency Management: Analysis of the Threat and Hazard Identification and Risk Assessment and the Hazard*

*Identification and Risk Assessment.* [e-Book]. (RAND Research Reports, RR-A2437-1). Santa Monica: RAND Corporation. DOI: https://doi.org/10.7249/RRA2437-1

Bennett, Brian T. (2018): *Understanding, Assessing, and Responding to Terrorism: Protecting Critical Infrastructure and Personnel.* (2nd ed.). Hoboken: John Wiley & Sons.

Best, Katharina Ley et al. (2020): *How to Analyze the Cyber Threat from Drones: Background, Analysis Frameworks, and Analysis Tools.* [e-Book]. (RAND Research Reports, RR-2972-RC). Santa Monica: RAND Corporation. DOI: https://doi.org/10.7249/RR2972

Biles, Clay W. (2023): *How to Stop a Hijacking: Critical Thinking in Civil Aviation Security.* Boca Raton: CRC Press. DOI: https://doi.org/10.4324/9781003336457

Bolz, Frank, Jr.; Dudonis, Kenneth J.; Schulz, David P. (2011): *The Counterterrorism Handbook: Tactics, Procedures, and Techniques, Fourth Edition*. (CRC Series in Practical Aspects of Criminal and Forensic Investigations). Boca Raton: CRC Press.

Bordeaux, John et al. (2023, November): *Identifying and Prioritizing Systemically Important Entities: Advancing Critical Infrastructure Security and Resilience*. [e-Book]. (RAND Research Reports, RR-A1512-1). Santa Monica: RAND Corporation. DOI: https://doi.org/10.7249/RRA1512-1

Brataas, Kjell (2018): *Crisis Communication: Case Studies and Lessons Learned from International Disasters*. Abingdon: Routledge. DOI: https://doi.org/10.4324/9781315368245

Brauner, Florian (2017): *Securing Public Transportation Systems: An Integrated Decision Analysis Framework for the Prevention of Terrorist Attacks as Example*. Wiesbaden: Springer Vieweg. DOI: https://doi.org/10.1007/978-3-658-15306-9

Bueger, Christian; Edmunds, Timothy (2024): *Understanding Maritime Security*. New York: Oxford University Press.

Bullock, Jane A.; Haddow, George D.; Coppola, Damon P. (2021): *Introduction to Homeland Security: Principles of All-Hazards Risk Management.* (6th ed.). Oxford: Butterworth-Heinemann.

Burke, Robert A. (2018): *Counter-Terrorism for Emergency Responders*. (3rd ed.). Boca Raton: CRC Press.

Čaleta, Denis; Powers, James F., Jr. (Eds.) (2020, September): *Cyber Terrorism and Extremism as Threat to Critical Infrastructure Protection.* [e-Book]. Ljubljana / Tampa: Ministry of Defense, Republic of Slovenia; Joint Special Operations University; Institute for Corporative, Security Studies. URL: https://dk.mors.si/info/index.php/sl/knjizne-novosti/495-cyber-terrorism-and-extremism-as-threat-to-critical-infrastructure-protection

Čaleta, Denis; Radović, Vesela (2015): *Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection*. (NATO Science for Peace and Security Series – D: Information and Communication Security, Vol. 39). Amsterdam: IOS Press.

Chatterjee, Samrat; Brigantic, Robert T.; Waterworth, Angela M. (Eds.) (2021): *Applied Risk Analysis for Guiding Homeland Security Policy and Decisions*. (Wiley Series in Operations Research and Management Science). Hoboken: John Wiley & Sons.

Collier, Stephen J.; Lakoff, Andrew (2021): *The Government of Emergency: Vital Systems, Expertise, and the Politics of Security.* (Princeton Studies in Culture and Technology). Princeton: Princeton University Press.

Coombs, W. Timothy; Holladay, Sherry J. (Eds.) (2023): *The Handbook of Crisis Communication.* (2nd ed.). (Handbooks in Communication and Media). Chichester: Wiley Blackwell. DOI: https://doi.org/10.1002/9781119678953

Coppola, Damon P.; Maloney, Erin K. (2017): *Communicating Emergency Preparedness: Practical Strategies for the Public and Private Sectors.* (2nd ed.). Abingdon: Routledge. DOI: https://doi.org/10.1201/9781315194714

Cordner, Gary; Wright, Martin (Eds.) (2024): *Routledge International Handbook of Policing Crises and Emergencies.* (Routledge International Handbooks). Abingdon: Routledge. DOI: https://doi.org/10.4324/9781003265214

Crowe, Adam S. (2015): *A Futurist's Guide to Emergency Management*. Boca Raton: CRC Press. DOI: https://doi.org/10.1201/b18476

Daponte, Pasquale; Klósak, Maciej; Bendarma, Amine (2024): *Modern Technologies Enabling Innovative Methods for Maritime Monitoring and Strengthening Resilience in Maritime*

*Critical Infrastructures*. (NATO Science for Peace and Security Series – D: Information and Communication Security, Vol. 65). Amsterdam: IOS Press.

Daponte, Pasquale; Paladi, Florentin (Eds.) (2023): *Monitoring and Protection of Critical Infrastructure by Unmanned Systems*. (NATO Science for Peace and Security Series – D: Information and Communication Security, Vol. 63). Amsterdam: IOS Press.

Deatherage, Robert H., Jr. (2022): *Survival Driving: Staying Alive on the World's Most Dangerous Roads.* (2nd ed). DOI: https://doi.org/10.4324/9781003093961

Dillon, Brian (2014): *Blackstone's Emergency Planning, Crisis and Disaster Management.* (2nd ed.). Oxford: Oxford University Press.

Di Pietro, Antonio; Martí, José (Eds.) (2024): *Critical Infrastructure: Modern Approach and New Developments.* [e-Book]. London: IntechOpen. DOI: https://doi.org/10.5772/intechopen.104070

Doro-on, Anna (2012): *Risk Assessment for Water Infrastructure Safety and Security*. Boca Raton: CRC Press. DOI: https://doi.org/10.1201/b11087

Doro-on, Anna M. (2014); *Risk Assessment and Security for Pipelines, Tunnels, and Underground Rail and Transit Operations*. Boca Raton: CRC Press. DOI: https://doi.org/10.1201/b17047

Dunn Cavelty, Myriam; Kristensen, Kristian Søby (Eds.) (2008): *Securing "the Homeland": Critical Infrastructure, Risk and (In)Security. (CSS Studies in Security and International Relations)*. Abingdon: Routledge.

Edwards, Frances L.; Goodrich, Daniel C. (2024): *Introduction to Transportation Security.* (2nd ed.). Boca Raton: CRC Press. DOI: https://doi.org/10.4324/9781003461722

Edwards, Matthew (Ed.) (2014): *Critical Infrastructure Protection*. (NATO Science for Peace and Security Series – E: Human and Societal Dynamics, Vol. 116). Amsterdam: IOS Press.

Egli, Dane S. (2015): *Beyond the Storms: Strengthening Homeland Security and Disaster Management to Achieve Resilience*. Abingdon: Routledge.

Elias, Bartholomew (2009): *Airport and Aviation Security: U.S. Policy and Strategy in the Age of Global Terrorism*. Boca Raton: CRC Press.

Eltaher, Hassan M. (2012): *Aviation and Maritime Security Intelligence*. Ottawa: E&W Communications.

Ercetin, Umran; Zuievska, Natalia; Vovk, Oksana (Eds.) (2024): *Critical Infrastructure Protection in Response to Terrorist Attacks*. (NATO Science for Peace and Security Series – E: Human and Societal Dynamics, Vol. 157). Amsterdam: IOS Press.

Erskine, Kevin L.; Volpi, Joy A. (2024): *Safety and Security for Churches and Other Places of Worship*. Boca Raton: CRC Press.

Evans, Carol V. (Ed.) (2022, November): *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency*. NATO COE-DAT Handbook 1. [e-Book]. Carlisle: US Army War College Press. URL: https://www.coedat.nato.int/publication/researches/12-Enabling%20NATO_s%20Collective%20Defense_%20Critical%20Infrastructure%20Secur.pdf

Fagel, Michael J. (Ed.) (2022): *Principles of Emergency Management and Emergency Operations Centers (EOC).* (2nd ed.). Boca Raton: CRC Press.

Farazmand, Ali (Ed.) (2016): *Global Cases in Best and Worst Practice in Crisis and Emergency Management*. Abingdon: Routledge.

Forest, James J. F. (Ed.) (2006): *Homeland Security: Protecting America's Targets*. (Volume 3: Critical Infrastructure). Westport: Praeger Security International.

Ganguly, Auroop Ratan; Bhatia, Udit; Flynn, Stephen E. (2018): *Critical Infrastructures Resilience: Policy and Engineering Principles*. New York: Routledge.

Gordon, Gary A.; Young, Richard R. (Eds.) (2020): *Intermodal Maritime Security: Supply Chain Risk Mitigation*. Amsterdam: Elsevier.

Harrison, John (2009): *International Aviation and Terrorism: Evolving Threats, Evolving Security. (Political Violence)*. Abingdon: Routledge.

Hellenberg, Timo et al. (Eds.) (2011): *Securing Air Traffic: Case CBRN Terrorism*. [e-Book]. Helsinki: Aleksanteri Institute, University of Helsinki. URL: https://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-4389

Hoffman, Bruce; Reinares, Fernando (Eds.) (2016): *The Evolution of the Global Terrorist Threat: From 9/11 to Osama bin Laden's Death*. (Columbia Studies in Terrorism and Irregular Warfare). New York: Columbia University Press.

Hollywood, John S. et al. (2024, March): *Improving the Security of Soft Targets and Crowded Places: A Landscape Assessment*. [e-Book]. (RAND Research Reports, RR-A2260-1). Santa Monica: RAND Corporation. DOI: https://doi.org/10.7249/RRA2260-1

Hornmoen, Harald; Backholm, Klas (Eds.) (2018): *Social Media Use in Crisis and Risk Communication: Emergencies, Concerns and Awareness*. Bingley: Emerald.

Houghton, Rick; Bennett, William (2021): *Emergency Characterization of Unknown Materials.* (2nd ed.). Boca Raton: CRC Press.

Jackson, Brian A. et al. (2012): *Efficient Aviation Security: Strengthening the Analytic Foundation for Making Air Transportation Security Decisions*. [e-Book]. (RAND Monographs, MG-1220-RC). Santa Monica: RAND Corporation. URL: https://www.rand.org/pubs/monographs/MG1220.html

Jin, Yan; Austin, Lucinda L. (Eds.) (2022): *Social Media and Crisis Communication*. (2nd ed.). Abingdon: Routledge. DOI: https://doi.org/10.4324/9781003043409

Jin, Yan; Reber, Bryan H.; Nowak, Glen J. (Eds.) (2020): *Advancing Crisis Communication Effectiveness: Integrating Public Relations Scholarship with Practice*. New York: Routledge. DOI: https://doi.org/10.4324/9780429330650

Johnson, Thomas A. (Ed.) (2015): *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare.* Boca Raton: CRC Press.

Kapoor, Manjari Khanna (2024): *Security by Design: Protecting Buildings and Public Places Against Crime and Terror*. Abingdon: Routledge. DOI: https://doi.org/10.1201/9781003395133

Kapucu, Naim; Boin, Arjen (Eds.) (2016): *Disaster and Crisis Management: Public Management Perspectives*. Abingdon: Routledge. DOI: https://doi.org/10.4324/9781315677545

Kapucu, Naim; Özerdem, Alpaslan; Sadiq, Abdul-Akeem (2022): *Managing Emergencies and Crises: Global Perspectives*. (2nd ed.). Burlington: Jones & Bartlett Learning.

Keupp, Marcus Matthias (Ed.) (2020): *The Security of Critical Infrastructures: Risk, Resilience and Defense.* (International Series in Operations Research & Management Science, Vol. 288). Cham: Springer Nature. DOI: https://doi.org/10.1007/978-3-030-41826-7

Khader, Majeed et al. (Eds.) (2019): *Learning from Violent Extremist Attacks: Behavioural Sciences Insights for Practitioners and Policymakers*. Singapore: World Scientific.

Kilroy, Richard J., Jr. (Eds.) (2018): *Threats to Homeland Security: Reassessing the All-Hazards Perspective.* (2nd ed.). Hoboken: Wiley.

Knox, Claire Connolly; Haupt, Brittany "Brie" (Eds.) (2020): *Cultural Competency for Emergency and Crisis Management: Concepts, Theories and Case Studies.* Abingdon: Routledge.

Kovács, Tünde Anna et al. (2024): *Critical Infrastructure Protection in the Light of the Armed Conflicts.* (Advanced Sciences and Technologies for Security Applications). Cham: Springer. DOI: https://doi.org/10.1007/978-3-031-47990-8

Kowalkowski, Stanisław; Kaźmierczak, Danuta; Paul, Salvin (Eds.) (2024): *Civil Protection Systems and Disaster Governance: A Cross-Regional Approach.* Cham: Palgrave Macmillan / Springer Nature. DOI: https://doi.org/10.1007/978-3-031-60167-5

Kruszka, Leopold; Klósak, Maciej; Muzolf, Paweł (2019): *Critical Infrastructure Protection: Best Practices and Innovative Methods of Protection*. (NATO Science for Peace and Security Series – D: Information and Communication Security, Vol. 52). Amsterdam: IOS Press.

Kruszka, Leopold et al. (2022): *Critical Energy Infrastructure Protection: Innovative Structures and Materials for Blast and Ballistic Protection.* (NATO Science for Peace and Security Series – D: Information and Communication Security, Vol. 60). Amsterdam: IOS Press.

Lawson, Chappell; Bersin, Alan; Kayyem, Juliette N. (Eds.) (2020): *Beyond 9/11: Homeland Security for the Twenty-First Century.* (Belfer Center Studies in International Security). Cambridge: The MIT Press. DOI: https://doi.org/10.7551/mitpress/13831.001.0001

Lazari, Alessandro; Mikac, Robert (Eds.) (2022): *The External Dimension of the European Union's Critical Infrastructure Protection Programme: From Neighbouring Frameworks to Transatlantic Cooperation*. Boca Raton: CRC Press. DOI: https://doi.org/10.4324/9781003273769

Lehr, Peter (2019): *Counter-Terrorism Technologies: A Critical Assessment. (Advanced Sciences and Technologies for Security Applications)*. Cham: Springer International. DOI: https://doi.org/10.1007/978-3-319-90924-0

Lewis, Ted G. (2020): *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation.* (3rd ed.). Hoboken: John Wiley & Sons.

Lewis, Ted G. (2024): *Critical Infrastructure Resilience and Sustainability Reader*. Hoboken: John Wiley & Sons.

Liu, Brooke Fisher; Mehta, Amisha M. (Eds.) (2024): *Routledge Handbook of Risk, Crisis, and Disaster Communication.* (Routledge Handbooks). Abingdon: Routledge. DOI: https://doi.org/10.4324/9781003363330

Logan, Caroline; Borum, Randy; Gill, Paul (Eds.) (2023): *Violent Extremism: A Handbook of Risk Assessment and Management.* London: UCL Press.

Lohmann, Sarah J. (Ed.) (2022, December): *Countering Terrorism on Tomorrow's Battlefield: Critical Infrastructure Security and Resiliency. NATO COE-DAT Handbook 2.* [e-Book]. Carlisle: US Army War College Press. URL: https://www.coedat.nato.int/publication/researches/15-Countering_TerrorismonTomorrowsBattlefield.pdf

Lum, Cynthia; Kennedy, Leslie W. (Eds.) (2012): *Evidence-Based Counterterrorism Policy.* (Springer Series on Evidence-Based Crime Policy). New York: Springer. DOI: https://doi.org/10.1007/978-1-4614-0953-3

Madigan, Michael L. (2018): *Handbook of Emergency Management Concepts: A Step-by-Step Approach*. Boca Raton: CRC Press.

Maguire, Mark; Westbrook, David A. (2021): *Getting Through Security: Counterterrorism, Bureaucracy, and a Sense of the Modern*. New York: Routledge.

McElreath, David H. et al. (2021): *Introduction to Homeland Security.* (3rd ed.). Boca Raton: CRC Press. DOI: https://doi.org/10.4324/9780429491962

McEntire, David A. (2019): *Introduction to Homeland Security: Understanding Terrorism Prevention and Emergency Management.* (2nd ed.). Hoboken: John Wiley & Sons.

McEntire, David A. (Ed.) (2023): *The Distributed Functions of Emergency Management and Homeland Security: An Assessment of Professions Involved in Response to Disasters and Terrorist Attacks*. Boca Raton: CRC Press.

Morag, Nadav (2011): *Comparative Homeland Security: Global Lessons*. Hoboken: Wiley & Sons.

Morewitz, Stephen (2019): *Kidnapping and Violence: New Research and Clinical Perspectives.* New York: Springer. DOI: https://doi.org/10.1007/978-1-4939-2117-1

Morral, Andrew R. et al. (2012): *Modeling Terrorism Risk to the Air Transportation System: An Independent Assessment of TSA's Risk Management Analysis Tool and Associated Methods.* [e-Book]. (RAND Monographs, MG-1241-TSA). Santa Monica: RAND Corporation. URL: https://www.rand.org/pubs/monographs/MG1241.html

Mueller, John; Stewart, Mark G. (2016): *Chasing Ghosts: The Policing of Terrorism*. New York: Oxford University Press.

Nemeth, Charles P. (2021): *Homeland Security: An Introduction to Principles and Practice.* (4th ed.) Boca Raton: CRC Press. DOI: https://doi.org/10.4324/9781003176053

Nemeth, Charles P. (2023): *Private Security: An Introduction to Principles and Practice*. (2nd ed.). Boca Raton: CRC Press. DOI: https://doi.org/10.4324/9781003217299

Niglia, Alessandro (Ed.) (2015): *The Protection of Critical Energy Infrastructure Against Emerging Security Challenges.* (NATO Science for Peace and Security Series – D: Information and Communication Security, Vol. 43). Amsterdam: IOS Press.

Niglia, Alessandro (2016): *Critical Infrastructure Protection Against Hybrid Warfare Security Related Challenges.* (NATO Science for Peace and Security Series – D: Information and Communication Security, Vol. 46). Amsterdam: IOS Press.

Nyampong, Yaw Otu Mankata (2013): *Insuring the Air Transport Industry Against Aviation War and Terrorism Risks and Allied Perils: Issues and Options in a Post-September 11, 2001 Environment*. Heidelberg: Springer. DOI: https://doi.org/10.1007/978-3-642-32433-8

Osiecki, Mateusz (2022): *International Legal Aspects of Aerial Terrorism: Methods of Law Enforcement in Aviation*. (Ius, Lex et Res Publica, Vol. 22). Berlin: Peter Lang.

Parks, Lisa (2018): *Rethinking Media Coverage: Vertical Mediation and the War on Terror*. Abingdon: Routledge.

Perdikaris, John (2014): *Physical Security and Environmental Protection.* Boca Raton: CRC Press. DOI: https://doi.org/10.1201/b16861

Pereira, Mauro Fernandes; Apostolakis, Apostolos (Eds.) (2021): *Terahertz (THz), Mid Infrared (MIR) and Near Infrared (NIR) Technologies for Protection of Critical Infrastructures Against Explosives and CBRN*. (NATO Science for Peace and Security Series B: Physics and Biophysics). Dordrecht: Springer. DOI: https://doi.org/10.1007/978-94-024-2082-1

Peritz, Aki J. (2021): *Disruption: Inside the Largest Counterterrorism Investigation in History*. Lincoln: Potomac Books.

Pesch-Cronin, Kelley A.; Marion, Nancy E. (2024): *Critical Infrastructure Protection, Risk Management, and Resilience: A Policy Perspective.* (2nd ed.). New York: Routledge. DOI: https://doi.org/10.4324/9781003434887

Phillips, Brenda D.; Landahl, Mark (2020): *Business Continuity Planning: Increasing Workplace Resilience to Disasters.* London: Butterworth-Heinemann. DOI: https://doi.org/10.1016/C2017-0-00385-3

Phillips, Brenda D.; Neal, David M.; Webb, Gary R. (2022): *Introduction to Emergency Management and Disaster Science*. (3rd ed.). New York: Routledge. DOI: https://doi.org/10.4324/9781003021919

Pomerleau, Pierre-Luc; Lowery, David L. (2020): *Countering Cyber Threats to Financial Institutions: A Private and Public Partnership Approach to Critical Infrastructure Protection.* Cham: Palgrave Macmillan / Springer Nature. DOI: https://doi.org/10.1007/978-3-030-54054-8

Popov, Oliver B.; Sukhostat, Lyudmila (2022): *Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems*. (NATO Science for Peace and Security Series – D: Information and Communication Security, Vol. 62). Amsterdam: IOS Press.

Price, Jeffrey C.; Forrest, J. S. (2024): *Practical Aviation Security: Predicting and Preventing Future Threats*. (4th ed.). Amsterdam: Butterworth-Heinemann.

Radosavljevic, Vladan; Banjari, Ines; Belojevic, Goran (Eds.) (2018): *Defence Against Bioterrorism: Methods for Prevention and Control*. (NATO Science for Peace and Security Series – A: Chemistry and Biology). Dordrecht: Springer. DOI: https://doi.org/10.1007/978-94-024-1263-5

Radvanovsky, Robert; Brodsky, Jacob (Eds.) (2016): *Handbook of SCADA/Control Systems Security*. (2nd ed.). Boca Raton: CRC Press. DOI: https://doi.org/10.1201/b19545

Radvanovsky, Robert S.; McDougall, Allan (2024): *Critical Infrastructure: Homeland Security and Emergency Preparedness*. (5th ed.). Boca Raton: CRC Press. DOI: https://doi.org/10.4324/9781003346630

Ramsay, James D.; Kiltz, Linda A. (Eds.) (2018): *Critical Issues in Homeland Security: A Casebook. New York: Routledge*. (Original work published 2014)

Rass, Stefan et al. (2020): *Cyber-Security in Critical Infrastructures: A Game-Theoretic Approach*. (Advanced Sciences and Technologies for Security Applications). Cham: Springer. DOI: https://doi.org/10.1007/978-3-030-46908-5

Ratnaweera, Harsha; Pivovarov, Oleksandr A. (Eds.) (2019): *Physical and Cyber Safety in Critical Water Infrastructure*. (NATO Science for Peace and Security Series – D: Information and Communication Security, Vol. 56). Amsterdam: IOS Press.

Romaniuk, Scott Nicholas; Catino, Martin Scott; Martin, C. Augustus (Eds.) (2023): *The Handbook of Homeland Security*. Boca Raton: CRC Press. DOI: https://doi.org/10.4324/9781315144511

Sadler, Anthony et al. (2016): *The 15:17 to Paris: The True Story of a Terrorist, a Train, and Three American Heroes*. New York: PublicAffairs.

Sageman, Marc (2019): *The London Bombings*. Philadelphia: University of Pennsylvania Press.

Schmid, Alex P. (Ed.) (2021): *Handbook of Terrorism Prevention and Preparedness.* [e-Book]. The Hague: ICCT Press. URL: https://www.icct.nl/handbook-terrorism-prevention-and-preparedness

Schweitzer, Glenn E. (2009): *Countering Terrorism: Biological Agents, Transportation Networks, and Energy Systems: Summary of a U.S.-Russian Workshop*. Washington, DC: National Academies Press.

Setola, Roberto et al. (Eds.) (2015): *Railway Infrastructure Security.* (Topics in Safety, Risk, Reliability and Quality, Vol. 27). Cham: Springer. DOI: https://doi.org/10.1007/978-3-319-04426-2

Sidorenko, Anatolie; Hahn, Horst (Eds.) (2020): *Functional Nanostructures and Sensors for CBRN Defence and Environmental Safety and Security.* (NATO Science for Peace and Security Series C: Environmental Security). Dordrecht: Springer. DOI: https://doi.org/10.1007/978-94-024-1909-2

Spellman, Frank R. (2007): *Transportation of Hazardous Materials Post-9/11*. Lanham: Government Institutes.

Spellman, Frank R. (2019): *Financial Services Sector Protection and Homeland Security.* Lanham: Bernan Press.

Spellman, Frank R.; Bieber, Revonna M. (2010): *Energy Infrastructure Protection and Homeland Security*. Lanham: Government Institutes.

Spellman, Frank R.; Stoudt, Melissa L. (2011): *Nuclear Infrastructure Protection and Homeland Security*. Lanham: Government Institutes.

Stedmon, Alex; Lawson, Glyn (Eds.) (2016): *Hostile Intent and Counter-Terrorism: Human Factors Theory and Application.* (Human Factors in Defence). Abingdon: Routledge.

Stern, Eric K. (2022): *Oxford Encyclopedia of Crisis Analysis*. (2 Vols). New York: Oxford University Press.

Stewart, Mark G.; Mueller, John (2018): *Are We Safe Enough? Measuring and Assessing Aviation Security*. Amsterdam: Elsevier. DOI: https://doi.org/10.1016/C2016-0-01215-9

Stewart, Mark G.; Rosowsky, David V. (Eds.) (2022): *Engineering for Extremes: Decision-Making in an Uncertain World.* (Springer Tracts in Civil Engineering). Cham: Springer Nature. DOI: https://doi.org/10.1007/978-3-030-85018-0

Stoddart, Kristan (2023): *Cyberwarfare: Threats to Critical Infrastructure*. (Palgrave Studies in Cybercrime and Cybersecurity). Cham: Palgrave Macmillan / Springer Nature. DOI: https://doi.org/10.1007/978-3-030-97299-8

Swanson, Charles (2021): *Professional Security Management: A Strategic Guide.* Abingdon: Routledge.

Tahmisoğlu, Mete; Özen, Çınar (2009): *Transportation Security Against Terrorism*. (NATO Science for Peace and Security Series – E: Human and Societal Dynamics, Vol. 54). Amsterdam: IOS Press.

Tatar, Unal; Gokce, Yasir; Gheorghe, Adrian V. (Eds.) (2017): *Strategic Cyber Defense: A Multidisciplinary Perspective*. (NATO Science for Peace and Security Series – D: Information and Communication Security, Vol. 48). Amsterdam: IOS Press.

Tatar, Unal et al. (Eds.) (2020): *Space Infrastructures: From Risk to Resilience Governance.* (NATO Science for Peace and Security Series – D: Information and Communication Security, Vol. 57) Amsterdam: IOS Press.

Theron, Paul; Bologna, Sandro (2013): *Critical Information Infrastructure Protection and Resilience in the ICT Sector*. Hershey: Information Science Reference.

Uusikylä, Petri; Jalonen, Harri; Jokip, Annukka (Eds.) (2024): *Information Resilience and Comprehensive Security: Challenges and Complexities in Wicked Environments*. (Information Technology and Global Governance). Cham: Palgrave Macmillan / Springer Nature. DOI: https://doi.org/10.1007/978-3-031-66196-9

Veilleux-Lepage, Yannick (2020): *How Terror Evolves: The Emergence and Spread of Terrorist Techniques*. London: Rowman & Littlefield International.

Vermetten, Eric et al. (Eds.) (2020): *Risk Management of Terrorism Induced Stress: Guidelines for the Golden Hours (Who, What and When)*. (NATO Science for Peace and Security Series – E: Human and Societal Dynamics, Vol. 148). Amsterdam: IOS Press.

Wengler, Patrick (2024): *Policing and CBRN Hazards: Advancing CBRN Competence in Police Education.* (Innovations in Policing). New York: Routledge. DOI: https://doi.org/10.4324/9781003340775

Wilkinson, Paul (Ed.) (2007): *Homeland Security in the UK: Future Preparedness for Terrorist Attack Since 9/11.* (Political Violence). Abingdon: Routledge.

Wilson, Jeremy M. et al. (2007, December): *Securing America's Passenger-Rail Systems.* [e-Book]. (RAND Monographs, MG-705-NIJ). Santa Monica: RAND Corporation. URL: https://www.rand.org/pubs/monographs/MG705.html

Wright, Stephen J. (2021): *Aviation Safety and Security: Utilizing Technology to Prevent Aircraft Fatality*. Boca Raton: CRC Press. DOI: https://doi.org/10.1201/9780429296451

Yates, Sheldon (Ed.) (2016): *National Critical Infrastructure Policy: Background and Select Cybersecurity Issues.* Hauppauge: Nova Science Publishers.

Zeigler, Sean M. et al. (2019): *Acquisition and Use of MANPADS Against Commercial Aviation: Risks, Proliferation, Mitigation, and Cost of an Attack*. [e-Book]. (RAND Research Reports, RR-4304-DOS). Santa Monica: RAND Corporation. DOI: https://doi.org/10.7249/RR4304

Zellen, Barry Scott (2013): *State of Recovery: The Quest to Restore American Security After 9/11.* London: Bloomsbury Academic.

## Theses

Adhiambo, Lynette Deborah (2016): *Effect of Terrorism on Air Transport Industry in Africa: A Case Study of Kenya*. (Master's Thesis, University of Nairobi, Nairobi, Kenya). URL: http://erepository.uonbi.ac.ke/handle/11295/99809

Ali, Ghanim Masood (2020, August): *A Deferred Model for Evaluating and Improving the Dubai Metro Train Security Management*. (Doctoral Thesis, Cardiff University, Cardiff, United Kingdom). DOI: https://doi.org/10.25401/cardiffmet.15062316.v1

Alkhaili, Khalifa (2015, October): *Building Disaster Resilience Within the Emirati Energy Sector and its Infrastructure Through a Comprehensive Strategic Mitigation Plan*. (Doctoral Thesis, University of Salford, Salford, United Kingdom). URL: https://salford-repository.worktribe.com/output/1410593/building-disaster-resilience-within-the-emirati-energy-sector-and-its-infrastructure-through-a-comprehensive-strategic-mitigation-plan

Alshawish, Ali (2021, October): *Risk-Based Security Management in Critical Infrastructure Organizations*. (Doctoral Thesis, University of Passau, Passau, Germany). URL: https://nbn-resolving.org/urn:nbn:de:bvb:739-opus4-10026

Bell, Alison Jane Cranston (2021, February): *The Insider Threat – Responding to Behavioural Indicators in Critical National Infrastructure Organsations*. (Doctoral Thesis, King's College London, London, United Kingdom). URL: https://kclpure.kcl.ac.uk/portal/en/studentTheses/the-insider-threat

Biskupovic, Sandra (2021): *Critical Infrastructure Resilience: Findings from a Systematic Review.* (Master's Thesis, University of Waterloo, Waterloo, Canada). URL: http://hdl.handle.net/10012/17358

Block, Molly Mae (2016, May): *Applying Situational Crime Prevention to Terrorism Against Airports and Aircrafts.* (Doctoral Thesis, University of Louisville, Louisville, United States). DOI: https://doi.org/10.18297/etd/2479

Borowsky, Paul M. (2009, May): *An Exploratory Analysis of the Psychological Dimensions of Airline Security and Correlates of Perceived Terrorism Threats: A Study of Active American Airlines Pilots.* (Master's Thesis, East Tennessee State University, Johnson City, United States). URL: https://dc.etsu.edu/etd/1824

Boutwell, Mark Allen (2019, December): *Exploring Industry Cybersecurity Strategy in Protecting Critical Infrastructure.* (Doctoral Thesis, Walden University, Minneapolis, United States). URL: https://scholarworks.waldenu.edu/dissertations/7965

Callander, Briony Elspeth (2015, December): *The Expansion of Counter-Terrorism in the EU Post-9/11: The Development of EU Aviation Security.* (Doctoral Thesis, University of Dundee, Dundee, Scotland, United Kingdom). URL: https://discovery.dundee.ac.uk/en/studentTheses/the-expansion-of-counter-terrorism-in-the-eu-post-911

Cohen, Samuel A. (2019, May): *Cybersecurity for Critical Infrastructure: Addressing Threats and Vulnerabilities in Canada.* (Master's Thesis, Missouri State University, Springfield, United States). URL: https://bearworks.missouristate.edu/theses/3340

Cousins, Joshua T. (2021, March): *Policing the Aerotropolis: A Model for Securing the Nation's*

*Large Airports.* (Master's Thesis, Naval Postgraduate School, Monterey, United States). URL: https://hdl.handle.net/10945/67120

Craft, LaMesha (2017, February): *Perceived Threats to Food Security and Possible Responses Following an Agro-Terrorist Attack.* (Doctoral Thesis, Walden University, Minneapolis, United States). URL: https://scholarworks.waldenu.edu/dissertations/3289

Duchesneau, Jacques (2015, April): *Aviation Terrorism: Thwarting High-Impact Low-Probability Attacks.* (Doctoral Thesis, Royal Military College of Canada, Kingston, Canada). URL: https://hdl.handle.net/11264/741

Egan, Taylor J. G. (2019, March): *Design and Control of Resilient Interconnected Microgrids for Reliable Mass Transit Systems.* (Master's Thesis, University of Ontario Institute of Technology, Oshawa, Canada). URL: https://hdl.handle.net/10155/1020

Ellis, Ryan Nelson (2011): *Networks, Deregulation, and Risk: The Politics of Critical Infrastructure Protection.* (Doctoral Thesis, University of California, San Diego, United States). URL: https://escholarship.org/uc/item/5b93r8tr

Feldman, Devin (2020, January): *Mitigating Potential Lone Wolf Terrorist Attacks Against Aviation Sector Infrastructure.* (Master's Thesis, Johns Hopkins University, Baltimore, United States). URL: http://jhir.library.jhu.edu/handle/1774.2/62331

Gonzalez, Manuel (2016): *The Question of Homeland Security in Rural America.* (Doctoral Thesis, Walden University, Minneapolis, United States). URL: https://scholarworks.waldenu.edu/dissertations/2261

Gottschalk, Jason Howard (2015, July): *Towards an Evaluation and Protection Strategy for Critical Infrastructure.* (Master's Thesis, Rhodes University, Grahamstown, South Africa). URL: http://hdl.handle.net/10962/d1018793

Gregson-Green, Lucy Elizabeth (2018, January): *Resilience, Security, and the Railway Station: A Unique Case Study of the Current and Future Resilience to Security Threats.* (Doctoral Thesis, Loughborough University, Loughborough, United Kingdom). URL: https://hdl.handle.net/2134/33411

Große, Christine (2020, April): *Towards Systemic Governance of Critical Infrastructure Protection: State and Relevance of a Swedish Case.* (Doctoral Thesis, Mid Sweden University, Sundsvall, Sweden). URL: https://urn.kb.se/resolve?urn=urn:nbn:se:miun:diva-39168

Guetler, Vivian Fiona (2022): *Exploring Cyberterrorism, Topic Models and Social Networks of Jihadists Dark Web Forums: A Computational Social Science Approach.* (Doctoral Thesis, West Virginia University, Morgantown, United States). DOI: https://doi.org/10.33915/etd.11253

Hamm, Dominik Ernst (2019, June): *Government Communication and Terrorist Organizations: Towards a Concept of "Crisis Communication" in Reaction to 21st Century Islamic Terrorist Attacks for Western Governments.* (Doctoral Thesis, Queen's University Belfast, Belfast, Northern Ireland). URL: https://pure.qub.ac.uk/en/studentTheses/government-communication-and-terrorist-organizations-towards-a-co

Harbour, Lance D. (2020, March): *Aligning the National Preparedness Goal and FEMA's National Preparedness Grants.* (Master's Thesis, Naval Postgraduate School, Monterey, United States). URL: https://hdl.handle.net/10945/64928

Harre-Young, Steven Nicholas (2012, April): *The Relative Performance and Consequences of Protecting Crowded Places from Vehicle-Borne Improvised Explosive Devices.* (Doctoral Thesis, Loughborough University, Loughborough, United Kingdom). URL: https://hdl.handle.net/2134/9757

Hodoh, Ofia B. (2015, Winter): *Utilizing the Risk Reduction Effectiveness and Capabilities Assessment Program to Emphasize Emergency Response Capabilities from a Food Terrorism Attack.* (Doctoral Thesis, University of Georgia, Athens, United States). URL: https://esploro.libs.uga.edu/esploro/outputs/9949334509202959

Hou, Guangyang (2019, Fall): *Multi-Scale Traffic Performance Modeling of Transportation Systems Subjected to Multiple Hazards.* (Doctoral Thesis, Colorado State University, Fort Collins, United States). URL: https://hdl.handle.net/10217/199830

Huff, Andrew G. (2014, March): *Enhancing Food Defense: Risk Managers' Perceptions, Criticality Assessments, and a Novel Method for Objectively Determining Food Systems' Criticality.* (Doctoral Thesis, University of Minnesota, Minneapolis, United States). URL: https://hdl.handle.net/11299/163766

Janczak-Hogarth, David Scott (2015, January): *A Bayesian Risk Assessment of the Saudi Arabian*

*Oil Supply Chain, 2001-2010.* (Doctoral Thesis, University of Exeter, Exeter, United Kingdom). URL: http://hdl.handle.net/10871/27142

Jashari, Linda (2018, March): *Soft Target Security: Environmental Design and the Deterrence of Terrorist Attacks on Soft Targets in Aviation Transportation.* (Master's Thesis, Naval Postgraduate School, Monterey, United States). URL: https://hdl.handle.net/10945/58317

Joyce, John P. (2011, March): *The Transportation Security Administration's Four Major Security Programs for Mass Transit—How They Can Be Improved to Address the Needs of Tier II Mass Transit Agencies.* (Master's Thesis, Naval Postgraduate School, Monterey, United States). URL: https://hdl.handle.net/10945/5755

Kaneberg, Elvira (2018): *Emergency Preparedness Management and Civil Defence in Sweden: An All-Hazards Approach for Developed Countries' Supply Chains.* (Doctoral Thesis, Jönköping University, Jönköping, Sweden). URL: https://urn.kb.se/resolve?urn=urn:nbn:se:hj:diva-39457

Kavousifard, Amir Hossein (2018, June): *Influence of Transverse Reinforcement on Bridge Column Resistance Against Blast Loads.* (Master's Thesis, Concordia University, Montreal, Canada). URL: https://spectrum.library.concordia.ca/id/eprint/984066

Kraidi, Layth (2020, May): *Development of an Integrated Risk Management Framework for Oil and Gas Pipeline Projects.* (Doctoral Thesis, Liverpool John Moores University, Liverpool, United Kingdom). DOI: https://doi.org/10.24377/LJMU.t.00014194

Kuligowski, Erica Dawn (2011): *Terror Defeated: Occupant Sensemaking, Decision-Making and Protective Action in the 2001 World Trade Center Disaster.* (Doctoral Thesis, University of Colorado, Boulder, United States). URL: https://scholar.colorado.edu/concern/graduate_thesis_or_dissertations/6t053g11g

Lee, Alfred B. (2021): *Probability Risk Assessments in Critical Infrastructure and Homeland Security*. (Doctoral Thesis, Liberty University, Lynchburg, United States). URL: https://digitalcommons.liberty.edu/doctoral/3865

Lin, Jiwei (2017): *Modelling of Critical Infrastructure Interdependencies for Vulnerability Analysis.* (Doctoral Thesis, Nanyang Technological University, Singapore, Republic of Singapore). URL: https://hdl.handle.net/10356/73356

Liquorie, Paul J. (2015, September): *Homeland Security Is Hometown Security: Comparison and Case Studies of Vertically Synchronized Catastrophe Response Plans*. (Master's Thesis, Naval Postgraduate School, Monterey, United States). URL: https://hdl.handle.net/10945/47297

Locke, Edward P. (2013, November): *The Use of Military Forces for Emergency Management: A Comparative Case Study of the United States and Israel.* (Doctoral Thesis, Capella University, Minneapolis, United States). URL: https://www.proquest.com/dissertations-theses/use-military-forces-emergency-management/docview/1473918429/se-2

Madia, James D. (2020, December): *Threat Assessment of Physical Attacks of Electric Infrastructure: How Do Terrorist Groups Select their Targets?* (Doctoral Thesis, University of Southern California, Los Angeles, United States). URL: https://www.hsdl.org/c/view?docid=850125

Malji, Andrea (2015): *Terrain, Trains, and Terrorism: The Influence of Geography on Terrorism in India.* (Doctoral Thesis, University of Kentucky, Lexington, United States). URL: https://uknowledge.uky.edu/polysci_etds/15

Massey, Patrick J. (2007, March): *Forging a Framework to Improve the Emergency Management Community's Ability to Respond to a Nuclear or Radiological Weapons Attack.* (Master's Thesis, Naval Postgraduate School, Monterey, United States). URL: https://hdl.handle.net/10945/3632

Mathew, Taj (2023, March): *Insider Threat: A Constant Problem with a Continuous Approach.* (Master's Thesis, Naval Postgraduate School, Monterey, United States). URL: https://www.hsdl.org/c/view?docid=878376

Matias, Diogo (2019, November): *An Empirical Game-Theoretic Approach to Airport Security Using Agent-Based Modelling and Simulation.* (Master's Thesis, Delft University of Technology, Delft, The Netherlands). URL: http://resolver.tudelft.nl/uuid:09434259-d628-4c74-8d73-f285030f6373

Matthews, Michael D. (2023, March): *We Are All Gonna Die: How the Weak Points of the Power Grid Leave the United States with an Unacceptable Risk.* (Master's Thesis, Naval Postgraduate School, Monterey, United States). URL: https://apps.dtic.mil/sti/trecms/pdf/AD1212940.pdf

McInerney, Joan (2009, March): *Strengthening Hospital Surge Capacity in the Event of Explosive or Chemical Terrorist Attacks.* (Master's Thesis, Naval Postgraduate School, Monterey, United States). URL: https://hdl.handle.net/10945/4806

Monson, Alex J. (2022, March): *Vulnerabilities to U.S. Waterway Infrastructure Impacting the Ability to Project Naval Power.* (Master's Thesis, Naval Postgraduate School, Monterey, United States). URL: https://hdl.handle.net/10945/69688

Olsvik, Elise Anonby (2015): *Challenges of Aviation Security Regulation in Norway Post 9/11*. (Doctoral Thesis, University of Stavanger, Stavanger, Norway). URL: http://hdl.handle.net/11250/2360216

Oroszi, Terry (2016): *A Pilot Study of High-Stakes Decision-Making for Crisis Leadership.* (Doctoral Thesis, Wright State University, Dayton, United States). URL: http://rave.ohiolink.edu/etdc/view?acc_num=wright1464709408

Ostergaard, Daniel J. (2016): *Business and Security in the Age of Terrorism: The Long-Term Effects of the September 11 Terrorist Attacks on Seaport Governance and Control.* (Doctoral Thesis, University of South Carolina, Columbia, United States). URL: https://scholarcommons.sc.edu/etd/3899

Pearson, Edward M. (2014, September): *The Consequences to National Security of Jurisdictional Gray Areas Between Emergency Management and Homeland Security.* (Master's Thesis, Naval Postgraduate School, Monterey, United States). URL: https://hdl.handle.net/10945/43977

Pepper, Matthew (2019, May): *Prehospital Response to Terrorism*. (Master's Thesis, Monash University, Melbourne, Australia). DOI: https://doi.org/10.26180/5cecae200f826

Place, David S.; Grubbs, Gregory A. (2009, June): *Empirical Evaluation of a Model of Team Collaboration Using Selected Transcripts from September 11, 2001.* (Master's Thesis, Naval Postgraduate School, Monterey, United States). URL: http://hdl.handle.net/10945/4682

Shwani, Hazim G. (2014, April): *Critical Infrastructure Protection.* (Master's Thesis, Utica College, Utica, United States). URL: https://www.proquest.com/dissertations-theses/critical-infrastructure-protection/docview/1534359368/se-2

Singh, Milan (2015, Summer): *The Bombing of Air India Flight 182: Demanding Justice, Public Inquiries, and Acts of Citizenship.* (Doctoral Thesis, Simon Fraser University, Burnaby, Canada). URL: https://summit.sfu.ca/item/15624

Strandh, Veronica (2015): *Responding to Terrorist Attacks on Rail Bound Traffic: Challenges for Inter-Organizational Collaboration.* (Doctoral Thesis, Umeå University, Umeå, Sweden). URL: https://urn.kb.se/resolve?urn=urn:nbn:se:umu:diva-107194

Thorne, Sara Eileen Bertin (2010, July): *Failures of Imagination: Terrorist Incident Response in the Context of Crisis Management.* (Doctoral Thesis, University of Portsmouth, Portsmouth, United Kingdom). URL: https://researchportal.port.ac.uk/en/studentTheses/failures-of-imagination

Vogiatzis, Dimitrios (2020, June): *The Way to the Promised Land or the Door to Armageddon: How Severe Are the Threats Against the Physical Security of Israeli Offshore Gas Platforms?* (Master's Thesis, Naval Postgraduate School, Monterey, United States). URL: https://hdl.handle.net/10945/65461

Williams, David S. (2010, December): *Improving the Security of the U.S. Aeronautical Domain: Adopting an Intelligence-Led, Risk-Based Strategy and Partnership.* (Master's Thesis, Naval Postgraduate School, Monterey, United States). URL: https://hdl.handle.net/10945/4960

Wood, Stephen (2018, May): *Passenger Experience of Security at UK Airports as a Result of Terrorism.* (Doctoral Thesis, Leeds Beckett University, Leeds, United Kingdom). URL: https://figshare.leedsbeckett.ac.uk/articles/thesis/Passenger_experience_of_security_at_UK_airports_as_a_result_of_terrorism/21502164/1

Zuber, Felix (2024): *Hacking the Airport X-Ray Machine*. (Master's Thesis, KTH Royal Institute of Technology, Stockholm, Sweden). URL: https://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-348491

## Journal Articles and Book Chapters

Abrahamsen, Eirik Bjorheim et al. (2017): A Framework for Selection of Strategy for Management of Security Measures. *Journal of Risk Research*, 20(3), 404-417. DOI: https://doi.org/10.1080/13669877.2015.1057205

Abrenio, Joseph; Gridley, Joel; Folk, Christopher (2017, Spring): Cyber Security and the Grid: We'll Leave the Lights on for You (If We Can). *Journal on Terrorism and Security Analysis,* 12, 1-33. URL: https://satsa.syr.edu/wp-content/uploads/2017/03/SATSA_2017_Vol_12_WebEdition.pdf

Abualnaja, Nader; Nayer, Gautam (2019, Fall): Do Muslim Americans Support Racial Profiling at Airports? *Islamophobia Studies Journal*, 5(1), 11-25. DOI: https://doi.org/10.13169/islastudj.5.1.0011

Albæk, Mette Mayli et al. (2020, May): The Controller: How Basil Hassan Launched Islamic State Terror into the Skies. *CTC Sentinel*, 13(5), 1-11. URL: https://ctc.westpoint.edu/wp-content/uploads/2020/05/CTC-SENTINEL-052020.pdf

Al-Dahash, Hajer; Kulatunga, Udayangani; Amaratunga, Dilanthi (2014): Evaluation of the System of Disaster Management Resulting from War Operations and Terrorism in Iraq. *Procedia Economics and Finance*, 18, 900-907. DOI: https://doi.org/10.1016/S2212-5671(14)01016-8 URL: http://eprints.hud.ac.uk/id/eprint/23029

Al-Gharibi, Mansoor; Warren, Matthew; Yeoh, William (2020): Risks of Critical Infrastructure Adoption of Cloud Computing by Government. *International Journal of Cyber Warfare and Terrorism*, 10(3), 47-58. DOI: https://doi.org/10.4018/IJCWT.2020070104

Anand, Manish (2018, January-February): A Systems Approach to Agricultural Biosecurity. *Health Security*, 16(1), 58-68. DOI: https://doi.org/10.1089/hs.2017.0035

Anghuwo, John Shivute; Imanuel, Peter; Nangolo, Sam Shimakeleni (2024, December): Anti-Unmanned Aerial Vehicle Detection System for Airports: Aviation and National Security Perspective. *Journal of Transportation Security*, 17(1), Article 12. DOI: https://doi.org/10.1007/s12198-024-00280-w

Aplin, Dylan; Rogers, Marian Brooke (2020, September): "Alert Not Alarm": The UK Experience of Public Counter-Terrorism Awareness and Training, with Explicit Reference to Project ARGUS. *The Police Journal: Theory, Practice and Principles*, 93(3), 167-182. DOI: https://doi.org/10.1177/0032258X19851537

Ard, Michael J. (2024): Intelligence Warning in the Corporate Sector: The 2013 In Amenas Terrorist Attack in Retrospect. *Journal of Policing, Intelligence and Counter Terrorism*, 19(4), 436-447. https://doi.org/10.1080/18335330.2023.2274614

Argomaniz, Javier (2015): The European Union Policies on the Protection of Infrastructure from Terrorist Attacks: A Critical Assessment. *Intelligence and National Security*, 30(2-3), 259-280. DOI: https://doi.org/10.1080/02684527.2013.800333

Argomaniz, Javier; Lehr, Peter (2016): Political Resilience and EU Responses to Aviation Terrorism. *Studies in Conflict & Terrorism*, 39(4), 363-379. DOI: https://doi.org/10.1080/1057610X.2016.1117334 URL: http://hdl.handle.net/10023/11390

Armenia, Stefano; Tsaples, Georgios (2018): Individual Behavior as a Defense in the "War on Cyberterror": A System Dynamics Approach. *Studies in Conflict & Terrorism*, 41(2), 109-132. DOI: https://doi.org/10.1080/1057610X.2016.1249775

Armenia, Stefano et al. (2018, January): A System Dynamics Simulation Tool for the Management of Extreme Events in Urban Transportation Systems. *International Journal of Critical Infrastructures*, 13(4), 329-353. DOI: https://doi.org/10.1504/IJCIS.2017.089241

Atwell, Julie (2020): Aviation and International Terrorism. In: Ben Saul (Ed.): *Research Handbook on International Law and Terrorism.* (2nd ed.). Cheltenham: Edward Elgar, 47-59.

Aydemir, Muzaffer; Ateş, Barış (2018): Employing Upper Echelon Approach to the Crisis Management Team Intervening in Terror Incidents and Regional Conflicts. *Defence Against Terrorism Review,* 10, 65-84. URL: https://www.coedat.nato.int/publication/datr/volumes/Datr_Vol.10.pdf

Aytekin, Akın; Dursun, Mahir (2023): Enhancing Cyber Defense and Resilience of Critical Infrastructures Against Terrorist Attacks. *Defence Against Terrorism Review*, 18, 45-66. URL: https://www.coedat.nato.int/publication/datr/volumes/datr18.pdf

Babb, Casey; Wilner, Alex (2019, December): Passwords, Pistols, and Power Plants: An Assessment of Physical and Digital Threats Targeting Canada's Energy Sector. *International Journal: Canada's Journal of Global Policy Analysis*, 74(4), 518-536. DOI: https://doi.org/10.1177/0020702019895263

Badami, Krishna G. et al. (2020, July): Analysis of Transfusion Therapy During the March 2019

Mass Shooting Incident in Christchurch, New Zealand. *Vox Sanguinis*, 115(5), 424-432. DOI: https://doi.org/10.1111/vox.12907

Baker, David Mc.A (2015): Tourism and Terrorism: Terrorists Threats to Commercial Aviation Safety & Security. *International Journal of Safety and Security in Tourism/Hospitality*, 12. URL: https://www.palermo.edu/Archivos_content/2015/economicas/journal-tourism/edicion12/02_Terrorism_Commercial_Aviation.pdf

Balogun, Taofeek Mobolarinwa; Bahşi, Hayretdin; Karabacak, Bilge (2017): Preliminary Analysis of Cyberterrorism Threats to Internet of Things (IoT) Applications. In: Maura Conway et al. (Eds.): *Terrorists' Use of the Internet: Assessment and Response*. (NATO Science for Peace and Security Series – E: Human and Societal Dynamics, Vol. 136). Amsterdam: IOS Press, 49-58. URL: https://fuse.franklin.edu/facstaff-pub/48

Balogun, Taofeek Mobolarinwa et al. (2023, September): A Comparative Framework for Cyber Threat Modelling: Case of Healthcare and Industrial Control Systems. *International Journal of Critical Infrastructures*, 19(5), 405-435. DOI: https://doi.org/10.1504/IJCIS.2023.133282

Bartolucci, Andrea; Magni, Michele (2023, December): Spontaneous Hospitalization in the Immediate Aftermath of the Manchester Arena Bombing. *Journal of Contingencies and Crisis Management*, 31(4), 627-634. DOI: https://doi.org/10.1111/1468-5973.12465

Basha, Saddiq (2023, September): "Death to the Grid": Ideological Narratives and Online Community Dynamics in Encouraging Far-Right Extremist Attacks on Critical Infrastructure. *Counter Terrorist Trends and Analyses*, 15(4), 17-24. URL: https://www.rsis.edu.sg/wp-content/uploads/2023/09/CTTA-September-2023.pdf

Bass, Sarah Bauerle et al. (2016, October): How Do Low-Literacy Populations Perceive "Dirty Bombs"? Implications for Preparedness Messages. *Health Security*, 14(5), 331-344. DOI: https://doi.org/10.1089/hs.2016.0037

Baucum, Matt et al. (2018, June): Modeling Public Responses to Soft-Target Transportation Terror. *Environment Systems and Decisions*, 38(2), 239-249. DOI: https://doi.org/10.1007/s10669-018-9676-7

Bayrak, Tuncay (2024, January): A Framework for a Mobile Knowledge Management Application for Crisis and Emergency Management. *Journal of Homeland Security and Emergency Management*, 21(1), 49-69. DOI: https://doi.org/10.1515/jhsem-2021-0021

Bearse, Ronald S. (2015): Protecting Critical Information Infrastructure from Terrorist Attacks and Other Threats: Strategic Challenges for NATO and its Partner Countries. In: Mehmet Nesip Ogun (Ed.): *Terrorist Use of Cyberspace and Cyber Terrorism: New Challenges and Responses*. (NATO Science for Peace and Security Series – D: Information and Communication Security, Vol. 42). Amsterdam: IOS Press, 29-44. DOI: https://doi.org/10.3233/978-1-61499-528-9-29

Bearse, Ronald S. (2021, June): Best Practices for Strengthening the Protection of NATO and Partner Nation Critical Infrastructure Against Terrorist Attacks: It Is All About the "How". In: Haldun Yalçınkaya (Ed.): *Good Practices in Counter Terrorism*. Ankara: Centre of Excellence Defence Against Terrorism (COE-DAT), 85-104. URL: https://www.coedat.nato.int/publication/researches/10-GoodPracticesIncounterTerrorism-I.pdf

Bearth, Angela et al. (2021, December): Increasing the Deterrence of Airport Security Checks by Managing Expectations Through Communication: A Hypothetical Scenario Experiment. *Journal of Transportation Security*, 14(3-4), 275-289. DOI: https://doi.org/10.1007/s12198-021-00240-8

Beckham, Tammy R.; Brake, David A.; Fine, Joshua B. (2018, March-April): Strengthening One Health Through Investments in Agricultural Preparedness. *Health Security*, 16(2), 92-107. DOI: https://doi.org/10.1089/hs.2017.0069

Berthold, Theresa et al. (2024, May): A National Disaster Medicine Quality Management Tool in an International Context – A Theoretical Study. *Journal of Homeland Security and Emergency Management*, 21(2), 189-207. DOI: https://doi.org/10.1515/jhsem-2021-0012

Besenyő, János; Márton, Krisztina; Shaffer, Ryan (2024): Hospital Attacks Since 9/11: An Analysis of Terrorism Targeting Healthcare Facilities and Workers. *Studies in Conflict & Terrorism*, 47(1), 36-59. DOI: https://doi.org/10.1080/1057610X.2021.1937821

Bier, Vicki M.; Kosanoglu, Fuat (2015, April): Target-Oriented Utility Theory for Modeling the Deterrent Effects of Counterterrorism. *Reliability Engineering & System Safety*, 136, 35-46. DOI: https://doi.org/10.1016/j.ress.2014.11.006

Biersteker, Erwin et al. (2017, April): Toward a Legal Perspective on Crisis Information Management: Legal Values and Privacy-Sensitive Information at Odds? *Journal of Homeland Security and Emergency Management,* 14(1), Article 20160060. DOI: https://doi.org/10.1515/jhsem-2016-0060

Birkett, David Michael (2017, May): Water Critical Infrastructure Security and its Dependencies. *Journal of Terrorism Research*, 8(2), 1-21. DOI: http://doi.org/10.15664/jtr.1289

Bjørnskov, Christian; Voigt, Stefan (2020, April): When Does Terror Induce a State of Emergency? And What Are the Effects? *Journal of Conflict Resolution*, 64(4), 579-613. DOI: https://doi.org/10.1177/0022002719865994

Bjørnskov, Christian; Voigt, Stefan (2022, May): Terrorism and Emergency Constitutions in the Muslim World. *Journal of Peace Research*, 59(3), 305-318. DOI: https://doi.org/10.1177/00223433211012445

Blackwood, Leda; Hopkins, Nick; Reicher, Stephen D. (2015, October): "Flying While Muslim": Citizenship and Misrecognition in the Airport. *Journal of Social and Political Psychology,* 3(2), 148-170. DOI: https://doi.org/10.5964/jspp.v3i2.375

Boin, Arjen; Smith, Denis (2006): Terrorism and Critical Infrastructures: Implications for Public–Private Crisis Management. *Public Money & Management*, 26(5), 295-304.

Booth, Alasdair; Bosher, Lee; Chmutina, Ksenia (2023, March): The Protection of Crowded Places from Terrorist Threats: Does Protective Security Advice Meet the Needs of Security Managers? *Security Journal*, 36(1), 141-164. DOI: https://doi.org/10.1057/s41284-022-00332-7

Bossong, Raphael (2015): The European Programme for the Protection of Critical Infrastructures – Meta-Governing a New Security Problem? In: Hans-Georg Ehrhart; Hendrik Hegemann; Martin Kahl (Eds.): *Putting Security Governance to the Test*. Abingdon: Routledge, 92-108.

Boyle, Philip J.; Speed, Shannon T. (2018, June): From Protection to Coordinated Preparedness: A Genealogy of Critical Infrastructure in Canada. *Security Dialogue*, 49(3), 217-231. DOI: https://doi.org/10.1177/0967010617748541

Brassett, James; Vaughan-Williams, Nick (2015, February): Security and the Performative Politics of Resilience: Critical Infrastructure Protection and Humanitarian Emergency Preparedness. *Security Dialogue*, 46(1), 32-50. DOI: https://doi.org/10.1177/0967010614555943

Brigantic, Robert et al. (2024, December): Aviation Security Screening Optimizer for Risk and Throughput (ASSORT). *Journal of Transportation Security*, 17(1), Article 22. DOI: https://doi.org/10.1007/s12198-024-00290-8

Brill, Alan; Smolanoff, Jason (2017): Hacking Back Against Cyberterrorists: Could you? Should you? *Defence Against Terrorism Review*, 9, 35-46. URL: https://www.coedat.nato.int/publication/datr/volumes/datr2017.pdf

Bronk, Chris; Conklin, Wm Arthur (2022): Who's in Charge and How Does it Work? US Cybersecurity of Critical Infrastructure. *Journal of Cyber Policy*, 7(2), 155-174. DOI: https://doi.org/10.1080/23738871.2022.2116346

Bueger, Christian; Liebetrau, Tobias (2021): Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network. *Contemporary Security Policy*, 42(3), 391-413. DOI: https://doi.org/10.1080/13523260.2021.1907129

Burato, Alessandro (2015): Crisis Management and Violent Radicalization: The Neglected Role of Risk Communication. In: Marco Lombardi et al. (Eds.): *Countering Radicalisation and Violent Extremism Among Youth to Prevent Terrorism.* (NATO Science for Peace and Security Series – E: Human and Societal Dynamics, Vol. 118). Amsterdam: IOS Press, 56-64. DOI: https://doi.org/10.3233/978-1-61499-470-1-56

Burns, Jeff (2017, Summer): Safe Travel in the Philippines in an Era of Terrorism and Kidnapping. *Journal of Counterterrorism and Homeland Security International*, 23(2), 10-15. URL: https://issuu.com/fusteros/docs/iacsp_magazine_v23n2_issuu

Busch, Nathan E.; Givens, Austen D. (2014): Public-Private Partnerships in Critical Infrastructure Protection. In: The Business of Counterterrorism: Public-Private Partnerships in Homeland Security. (*Terrorism Studies*, Vol. 4). New York: Peter Lang, 49-86.

Cain, Lauren; Herovic, Emina; Wombacher, Kevin (2021, September): "You Are Here": Assessing the Inclusion of Maps in a Campus Emergency Alert System. *Journal of Contingencies and Crisis Management*, 29(3), 332-340. DOI: https://doi.org/10.1111/1468-5973.12358

Caşin, Mesut Hakkı (2016): Critical Energy Infrastructure Protection Against Terrorist Attacks in the Context of Gas and Oil Pipelines: The Turkish Case. *Defence Against Terrorism Review*, 8, 37-52. URL: https://www.coedat.nato.int/publication/datr/volumes/datr8-2016.pdf

Cazalas, Edward (2018, December): Defending Cities Against Nuclear Terrorism: Analysis of a Radiation Detector Network for Ground Based Traffic. *Homeland Security Affairs*, 14, Article 10. URL: https://www.hsaj.org/articles/14715

Chaurasia, Priyanka et al. (2016): Countering Terrorism, Protecting Critical National Infrastructure and Infrastructure Assets Through the Use of Novel Behavioral Biometrics. *Behavioral Sciences of Terrorism and Political Aggression*, 8(3), 197-211. DOI: https://doi.org/10.1080/19434472.2016.1146788

Christello, Gabrielle (2024, July): The Rise of Iran's Cyber Capabilities and the Threat to U.S. Critical Infrastructure. *Georgetown Security Studies Review*, 12(1), 12-22. URL: https://repository.library.georgetown.edu/handle/10822/1088844

Christensen, Tom; Lægreid, Per; Rykkja, Lise H. (2023): How to Balance Individual Rights and Societal Security? The View of Civil Servants. *Studies in Conflict & Terrorism*, 46(7), 1150-1166. DOI: https://doi.org/10.1080/1057610X.2018.1538187

Chun-lin, Liu; Gunaratna, Rohan (2022): Lebanon's Single Most Destructive Explosion – Terrorists Plan to Copy and Provision Against Such Accidents. *Journal of Applied Security Research*, 17(3), 310-331. DOI: https://doi.org/10.1080/19361610.2021.1873681

Cinturati, Frank (2014): The Bioterrorism Act and Water Utilities Protection: How to Proceed from Policy to Practice. *Journal of Applied Security Research*, 9(1), 97-108. DOI: https://doi.org/10.1080/19361610.2014.851575

Clarke, Colin P. et al. (2023, May): The Targeting of Infrastructure by America's Violent Far-Right. *CTC Sentinel*, 16(5), 26-32. URL: https://ctc.westpoint.edu/wp-content/uploads/2023/05/CTC-SENTINEL-052023.pdf

Condell, Joan et al. (2018): Automatic Gait Recognition and its Potential Role in Counterterrorism. *Studies in Conflict & Terrorism*, 41(2), 151-168. DOI: https://doi.org/10.1080/1057610X.2016.1249777

Cordova, Amado (2022, December): Technologies for Primary Screening in Aviation Security. *Journal of Transportation Security*, 15(3-4), 141-159. DOI: https://doi.org/10.1007/s12198-022-00248-8

Daly, Andrew (2012): Using Ordered Attitudinal Indicators in a Latent Variable Choice Model: A Study of the Impact of Security on Rail Travel Behaviour. *Transportation*, 39(2), 267-297. DOI: https://doi.org/10.1007/s11116-011-9351-z

Davis, Xiaohong M.; Rouse, Edward N.; Stampley, Chaunté (2021, January): Preparing the CDC Public Health Workforce for Emergency Response. *Journal of Homeland Security and Emergency Management*, 18(1), 1-21. DOI: https://doi.org/10.1515/jhsem-2019-0021

De Cillis, Francesca et al. (2013, August): Analysis of Criminal and Terrorist Related Episodes in Railway Infrastructure Scenarios. *Journal of Homeland Security and Emergency Management*, 10(2), 447-476. DOI: https://doi.org/10.1515/jhsem-2013-0003

Demir, Mustafa; Guler, Ahmet; Ozer, Murat (2024): Predictors of Successful Terrorism Incidents. *Behavioral Sciences of Terrorism and Political Aggression*, 16(4), 482-510. DOI: https://doi.org/10.1080/19434472.2022.2130396

Dillon, Robin L.; Burns, William J.; John, Richard S. (2018, September): Insights for Critical Alarm-Based Warning Systems from a Risk Analysis of Commercial Aviation Passenger Screening. *Decision Analysis,* 15(3), 154-173. DOI: https://doi.org/10.1287/deca.2018.0369

Dmitrieva, Aleksandra M.; Meloy, J. Reid (2022): Troubled Waters: Domestic Terrorism Threat in the U.S. Coast Guard and the TRAP-18. *Journal of Threat Assessment and Management*, 9(3), 153-170. DOI: https://doi.org/10.1037/tam0000170 URL: https://drreidmeloy.com/wp-content/uploads/2022/01/2021_TroubledWatersDomesticTerrorism.pdf

Drury, John; Cocking, Chris; Reicher, Steve (2009, March): The Nature of Collective Resilience: Survivor Reactions to the 2005 London Bombings. *International Journal of Mass Emergencies and Disasters*, 27(1), 66-95. DOI: https://doi.org/10.1177/028072700902700104

Dudenhoeffer, Donald D. (2020): Day of the Drone: Protecting Critical Infrastructure from Terrorist Use of Unmanned Aerial Systems. In: Alan Brill; Kristina Misheva; Metodi Hadji-Janev

(Eds.): *Toward Effective Cyber Defense in Accordance with the Rules of Law.* (NATO Science for Peace and Security Series – E: Human and Societal Dynamics, Vol. 149). Amsterdam: IOS Press, 17-31. DOI: https://doi.org/10.3233/NHSDP200038

Duggan, James M.; Petrozzelli, John; Slattery, Jay (2023): Implementing NIMS: Lessons Learned from the Boston Marathon Bombing. *Journal of Strategic Security*, 16(3), Article 5. DOI: https://doi.org/10.5038/1944-0472.16.3.2139

Ekhomu, Ona (2020): Infrastructure Attacks. In: *Boko Haram: Security Considerations and the Rise of an Insurgency*. Boca Raton: CRC Press, 131-148.

Ellis, Cali M.; McDaniel, Michael C. (2013, April): Texas Takes on the TSA: The Constitutional Fight Over Airport Security. *Journal of Homeland Security and Emergency Management*, 10(1), 209-229. DOI: https://doi.org/10.1515/jhsem-2012-0068

Elsass, H. Jaymi; McKenna, Joseph M.; Schildkraut, Jaclyn (2016, November): Rethinking Crisis Communications on Campus: An Evaluation of Faculty and Staff Perceptions About Emergency Notification Systems. *Journal of Homeland Security and Emergency Management*, 13(3), 329-349. DOI: https://doi.org/10.1515/jhsem-2016-0047

Ergün, Nalan; Açıkel, Birsen Yörük; Turhan, Uğur (2017, January): The Appropriateness of Today's Airport Security Measures in Safeguarding Airline Passengers. *Security Journal*, 30(1), 89-105. DOI: https://doi.org/10.1057/sj.2014.41

Eriksson, Mats (2024, March): Living a "Digital Life" and Ready to Cope with Crises? Highlighting Young Adults' Conceptions of Crisis and Emergency Preparedness. *Journal of Contingencies and Crisis Management*, 32(1), Article e12498. DOI: https://doi.org/10.1111/1468-5973.12498

Evans, Carol V. (2020, May): Future Warfare: Weaponizing Critical Infrastructure. *Parameters*, 50(2), 35-42. DOI: https://doi.org/10.55540/0031-1723.1017

Farhat, Hassan et al. (2024, March): Exploring Attitudes Towards Health Preparedness in the Middle East and North Africa Against Chemical, Biological, Radiological, and Nuclear Threats: A Qualitative Study. *Journal of Contingencies and Crisis Management*, 32(1), Article e12509. DOI: https://doi.org/10.1111/1468-5973.12509

Farhat, Hassan et al. (2024, May-June): Perspectives on Preparedness for Chemical, Biological, Radiological, and Nuclear Threats in the Middle East and North Africa Region: Application of Artificial Intelligence Techniques. *Health Security*, 22(3), 190-202. DOI: https://doi.org/10.1089/hs.2023.0093

Fianyi, Israel; Zia, Tanveer (2016): Biometric Technology Solutions to Countering Today's Terrorism. *International Journal of Cyber Warfare and Terrorism*, 6(4), 28-40. DOI: https://doi.org/10.4018/IJCWT.2016100103

Fiondella, Lance et al. (2013, April): Security and Performance Analysis of a Passenger Screening Checkpoint for Mass-Transit Systems. *Homeland Security Affairs,* Suppl. 6, Article 3. URL: https://www.hsaj.org/articles/241

Florido-Benítez, Lázaro (2024, December): The Types of Hackers and Cyberattacks in the Aviation Industry. *Journal of Transportation Security*, 17(1), Article 13. DOI: https://doi.org/10.1007/s12198-024-00281-9

Forest, James J. F. (2007, December): The Modern Terrorist Threat to Aviation Security. *Perspectives on Terrorism,* 1(6), 10-13. URL: https://pt.icct.nl/article/modern-terrorist-threat-aviation-security

Fox, Sarah Jane (2021): Past Attacks, Future Risks: Where Are We 20-Years After 9/11? *Journal of Strategic Security*, 14(3), Article 6. DOI: https://doi.org/10.5038/1944-0472.14.3.1964

Freudenberg, Dirk (2023): Hybrid Loans and Tactics of Jihadism: Will Hybridity Remain the Narrative of Convergent, Politically Motivated Violence? In: Nicolas Stockhammer (Ed.): *Routledge Handbook of Transnational Terrorism*. (Routledge Handbooks). Abingdon: Routledge, Chapter 27.

Gabbe, Belinda J. et al. (2020, April): Survey of Major Trauma Centre Preparedness for Mass Casualty Incidents in Australia, Canada, England and New Zealand. *eClinicalMedicine*, 21, Article 100322. DOI: https://doi.org/10.1016/j.eclinm.2020.100322

Gartenstein-Ross, Daveed; Joscelyn, Thomas (2022): The Unfriendly Skies: Plots Against Aviation. In: *Enemies Near and Far: How Jihadist Groups Strategize, Plot, and Learn*. (Columbia Studies in Terrorism and Irregular Warfare). New York: Columbia University Press, 70-106.

Giacomello, Giampiero (2023): Research Note: More Bucks, Still No Bangs? Why a Cost-Benefit

Analysis of Cyberterrorism Still Holds True. *Studies in Conflict & Terrorism*, 46(8), 1508-1517. DOI: https://doi.org/10.1080/1057610X.2020.1822591

Gibson, Stacey; Lemyre, Louise; Lee, Jennifer E. C. (2015): Predicting Emergency Response Intentions Among the Canadian Public in the Context of Terrorism Threats: Examining Sociodemographics and the Mediating Role of Risk Perception. *Human and Ecological Risk Assessment*, 21(1), 205-226. DOI: https://doi.org/10.1080/10807039.2014.902683

Giesecke, James A. et al. (2015): Regional Dynamics Under Adverse Physical and Behavioral Shocks: The Economic Consequences of a Chlorine Terrorist Attack in the Los Angeles Financial District. In: Peter Nijkamp; Adam Rose; Karima Kourtit (Eds.): *Regional Science Matters: Studies Dedicated to Walter Isard*. Cham: Springer, 319-350. DOI: https://doi.org/10.1007/978-3-319-07305-7_16

Gill, Charlotte et al. (2021, June): "Translational Criminology" in Action: A National Survey of TSA's Playbook Implementation at U.S. Airports. *Security Journal*, 34(2), 319-339. DOI: https://doi.org/10.1057/s41284-019-00225-2

Gnatyuk, Sergiy (2016): Meeting Security Challenges Through Data Analytics and Decision Support. In: Elisa Shahbazian; Galina Rogova (Eds.): *Meeting Security Challenges Through Data Analytics and Decision Support*. (NATO Science for Peace and Security Series – D: Information and Communication Security, Vol. 47). Amsterdam: IOS Press, 308-316. DOI: https://doi.org/10.3233/978-1-61499-716-0-308

Goertz, Stefan (2018, March): TerrorMANV – Massenanfall von Verletzten bei Terrorlagen. *Die Kriminalpolizei*, März 2018. URL: https://www.kriminalpolizei.de/ausgaben/2018/detailansicht-2018/artikel/terrormanv-massenanfall-von-verletzten-bei-terrorlagen.html

Grant, Matthew J.; Stewart, Mark G. (2017, June): Benefit of Distributed Security Queuing for Reducing Risks Associated with Improvised Explosive Device Attacks in Airport Terminals. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part B: Mechanical Engineering*, 3(2), Article 021003. DOI: https://doi.org/10.1115/1.4035730

Gücüyener, Ayhan (2018): Cyber Terrorism and Energy Security: A Growing Threat Imperils Entire Regions. *per Concordiam*, 8(4), 58-61. URL: http://perconcordiam.com/perCon_V8N4_ENG.pdf

Guohui, Li et al. (2014): Study on Correlation Factors that Influence Terrorist Attack Fatalities Using Global Terrorism Database. *Procedia Engineering*, 84, 698-707. DOI: https://doi.org/10.1016/j.proeng.2014.10.475

Haase, Thomas W.; Demiroz, Fatih (2020, May): Considerations of Resilience in the Homeland Security Literature: Towards Conceptual Convergence? *Journal of Homeland Security and Emergency Management*, 17(2), Article 20180078. DOI: https://doi.org/10.1515/jhsem-2018-0078

Haddow, George D.; Bullock, Jane A.; Coppola, Damon P. (2020): Emergency Management and the Terrorist Threat. In: *Introduction to Emergency Management*. (7th ed.). Oxford: Butterworth-Heinemann, 403-466.

Hambridge, Nicholas B.; Howitt, Arnold M.; Giles, David W. (2017, April): Coordination in Crises: Implementation of the National Incident Management System by Surface Transportation Agencies. *Homeland Security Affairs*, 13(2), Article 2. DOI: https://www.hsaj.org/articles/13773

Harwood, Shawn; Porter, Wayne (2020, August): The Case for Adaptive SOPs in Complex Crises and Unpredictable Operating Environments. *Homeland Security Affairs*, 16(5), Article 5. URL: https://www.hsaj.org/articles/16105

Hasisi, Badi et al. (2020, September): Concentrated and Close to Home: The Spatial Clustering and Distance Decay of Lone Terrorist Vehicular Attacks. *Journal of Quantitative Criminology*, 36(3), 607-645. DOI: https://doi.org/10.1007/s10940-019-09414-z

Hastings, Justin V.; Chan, Ryan J. (2013): Target Hardening and Terrorist Signaling: The Case of Aviation Security. *Terrorism and Political Violence*, 25(5), 777-797. DOI: https://doi.org/10.1080/09546553.2012.699906

Haugstvedt, Håvard (2024, March): Still Aiming at the Harder Targets: An Update on Violent Non-State Actors' Use of Armed UAVs. *Perspectives on Terrorism*, 18(1), 132-143. URL: https://pt.icct.nl/sites/default/files/2024-03/Research%20note%20template%202024_Hausgstved_0.pdf

Haupt, Brittany (2021, May): The Use of Crisis Communication Strategies in Emergency

Management. *Journal of Homeland Security and Emergency Management,* 18(2), 125-150. DOI: https://doi.org/10.1515/jhsem-2020-0039

Hedel, Ralf et al. (2018, October): Assessment of the European Programme for Critical Infrastructure Protection in the Surface Transport Sector. *International Journal of Critical Infrastructures*, 14(4), 311-335. DOI: https://doi.org/10.1504/IJCIS.2018.095616

Hemme, Kris (2015, Fall): Critical Infrastructure Protection: Maintenance Is National Security. *Journal of Strategic Security*, 8(3, Suppl.), Article 3. DOI: https://doi.org/10.5038/1944-0472.8.3S.1471

Hildebrand, Sean (2015, May): Coerced Confusion? Local Emergency Policy Implementation After September 11. *Journal of Homeland Security and Emergency Management*, 12(2), 273-298. DOI: https://doi.org/10.1515/jhsem-2014-0054

Hildebrand, Sean (2020, September): Representative Bureaucracy in Emergency Management: Attitudes About Contemporary Emergency Management Policy and Politics in Local Agencies. *Journal of Homeland Security and Emergency Management*, 17(3), Article 20190009. DOI: https://doi.org/10.1515/jhsem-2019-0009

Hodgson, Luke (2021, April): How Violent Attacks Are Changing the Demands of Mass Casualty Incidents: A Review of the Challenges Associated with Intentional Mass Casualty Incidents. *Homeland Security Affairs*, 17, Article 1. URL: https://www.hsaj.org/articles/16880

Hodwitz, Omi (2020): Threats to Aviation: Modeling Effectiveness. *Journal of Applied Security Research*, 15(3), 385-407. DOI: https://doi.org/10.1080/19361610.2019.1710093

Hodwitz, Omi; Tracy, Hailee (2020): President Trump's Travel Ban: Inciting or Deterring Terrorism? *Behavioral Sciences of Terrorism and Political Aggression*, 12(4), 292-306. DOI: https://doi.org/10.1080/19434472.2019.1701525

Hoijtink, Marijn (2015): Performativity and the Project: Enacting Urban Transport Security in Europe. *Critical Studies on Terrorism*, 8(1), 130-146. DOI: https://doi.org/10.1080/17539153.2015.1005937

Holgersson, Annelie (2016): Review of On-Scene Management of Mass-Casualty Attacks. *Journal of Human Security*, 12(1), 91-111. DOI: https://doi.org/10.12924/johs2016.12010091

Holgersson, Annelie; Björnstig, Ulf (2014, March): Mass-Casualty Attacks on Public Transportation. *Journal of Transportation Security*, 7(1), 1-16. DOI: https://doi.org/10.1007/s12198-013-0125-z

Holgersson, Annelie et al. (2020, April): Emergency Medical Response in Mass Casualty Tunnel Incidents—with Emphasis on Prehospital Care. *Journal of Human Security*, 16(1), 3-15. DOI: https://doi.org/10.12924/johs2020.16010003

Hopfner, Benedikt (2016): Protecting Europe's Critical Infrastructure. *per Concordiam*, 7(4), 58-63. URL: https://perconcordiam.com/perCon_V7N4_ENG_hires.pdf

Horner, Matthew (2018, April): SCADA Fusion with Commercial Fission. *Homeland Security Affairs*, 14, Article 4. URL: https://www.hsaj.org/articles/14317

Hsu, Henda Y.; Apel, Robert (2016): A Situational Model of Displacement and Diffusion Following the Introduction of Airport Metal Detectors. In: Joshua Freilich; Gary LaFree (Eds.): *Criminology Theory and Terrorism: New Applications and Approaches.* Abingdon: Routledge, 29-52.

Hsu, Henda Y.; McDowall, David (2017, November): Does Target-Hardening Result in Deadlier Terrorist Attacks Against Protected Targets? An Examination of Unintended Harmful Consequences. *Journal of Research in Crime and Delinquency*, 54(6), 930-957. DOI: https://doi.org/10.1177/0022427817719309

Hughes, Geraint (2014, September): Skyjackers, Jackals and Soldiers: British Planning for International Terrorist Incidents During the 1970s. *International Affairs*, 90(5), 1013-1031. DOI: https://doi.org/10.1111/1468-2346.12154

Huttunen, Mikko (2019, December): Civil Unmanned Aircraft Systems and Security: The European Approach. *Journal of Transportation Security*, 12(3-4), 83-101. DOI: https://doi.org/10.1007/s12198-019-00203-0

Hwang, Seongwon; Cho, Namsuk (2019, February): Optimisation Models for Critical Infrastructure Protection, Rebuilding, and Interdependency in the Event of Mass Destruction. *International Journal of Critical Infrastructures*, 15(2), 136-162. DOI: https://doi.org/10.1504/IJCIS.2019.098836

Ismail, Suhaila; Sitnikova, Elena; Slay, Jill (2016): SCADA Systems Cyber Security for Critical Infrastructures: Case Studies in Multiple Sectors. *International Journal of Cyber Warfare and Terrorism*, 6(3), 79-95. DOI: https://doi.org/10.4018/IJCWT.2016070107

Jaafar, Hadi; Sujud, Lara; Woertz, Eckart (2022): Scorched Earth Tactics of the "Islamic State" After its Loss of Territory: Intentional Burning of Farmland in Iraq and Syria. *Regional Environmental Change*, 22(4), Article 120. DOI: https://doi.org/10.1007/s10113-022-01976-2

Jackson, Brian A.; Chan, Edward W.; Latourrette, Tom (2012, March): Assessing the Security Benefits of a Trusted Traveler Program in the Presence of Attempted Attacker Exploitation and Compromise. *Journal of Transportation Security*, 5(1), 1-34. DOI: https://doi.org/10.1007/s12198-011-0077-0

Jamil, Uzma (2017, Fall): Can Muslims Fly? The No Fly List as a Tool of the "War on Terror". *Islamophobia Studies Journal*, 4(1), 72-86. DOI: https://doi.org/10.13169/islastudj.4.1.0072

Jasani, Gregory N. et al. (2023, March-April): Terrorist Attacks Against Firefighters, 1970-2019. *Health Security,* 21(2), 141-145. DOI: https://doi.org/10.1089/hs.2022.0075

Jonathan-Zamir, Tal; Hasisi, Badi; Margalioth, Yoram (2016, September): Is It the What or the How? The Roles of High-Policing Tactics and Procedural Justice in Predicting Perceptions of Hostile Treatment: The Case of Security Checks at Ben-Gurion Airport, Israel. *Law & Society Review*, 50(3), 608-636. DOI: https://doi.org/10.1111/lasr.12216

Jupe, Louise Marie; Keatley, David Adam (2020, December): Airport Artificial Intelligence Can Detect Deception: Or Am I Lying? *Security Journal*, 33(4), 622-635. DOI: https://doi.org/10.1057/s41284-019-00204-7

Juvan, Jelena; Prezelj, Iztok; Kopač, Erik (2021, September): Public Dilemmas About Security Measures in the Field of Civil Aviation. *Security Journal*, 34(3), 410-428. DOI: https://doi.org/10.1057/s41284-020-00240-8

Kaczmarek, Krzysztof; Karpiuk, Mirosław; Soler, Urszula (2024): The Potential Use of Artificial Intelligence in Crisis Management. *Sicurezza, Terrorismo e Società*, 20, 141-151. URL: https://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2024/12/008_SicTerSoc_20_Kaczmarek_et_al.pdf

Kamil, Ismaila Adeniyi; Ogundoyin, Sunday Oyinlola (2018): A Privacy-Preserving Passenger Information Management Scheme for Road Transport System in Nigeria. *Journal of Applied Security Research*, 13(4), 502-531. DOI: https://doi.org/10.1080/19361610.2018.1498268

Kaneda, Yudai et al. (2023): The Importance of the Taliban and the International Community Collaboration in Building Support Systems for Experts Working in Earthquake-Affected Areas in Afghanistan—Perspectives from a Triple Disaster Experience in Fukushima. *Disaster Medicine and Public Health Preparedness*, 17, Article E265. DOI: https://doi.org/10.1017/dmp.2022.260

Karpiuk, Mirosław (2022): Crisis Management vs. Cyber Threats. *Sicurezza, Terrorismo e Società*, 16, 113-123. URL: https://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2022/12/SicTerSoc16-Karpiuk-Crisis-management-vs.-cyber-threats.pdf

Kaszeta, Dan (2017, March): Protecting Against Chemical and Biological Risks to Office Buildings. *Journal of Terrorism & Cyber Insurance*, 1(2), 37-44. URL: http://docs.wixstatic.com/ugd/7cfaab_dbd9c13d3c3d42049cf078a3e876b28a.pdf

Kaunert, Christian; Callander, Briony; Léonard, Sarah (2023): The Collective Securitization of Aviation in the European Union Through Association with Terrorism. In: Christian Kaunert; Sarah Léonard (Eds.): *Collective Securitization and Crisification of EU Policy Change: Two Decades of EU Counterterrorism Policy.* Abingdon: Routledge, 61-78.

Kayhan, Selçuk; Ergün, Nalan; Gerede, Ender (2018, April): Research Determining Issues on the Administrative Success of Security Services at Civil Airports in Turkey. *Security Journal*, 31(2), 470-500. DOI: https://doi.org/10.1057/s41284-017-0111-4

Khalid, Nazery (2013): Battening Down the Hatches: Some Reflections on Protecting the Maritime Supply Chain from Maritime Terrorism. *SEARCCT's Selection of Articles*, 1, 17-29. URL: https://www.searcct.gov.my/wp-content/uploads/2020/03/SEARCCTS-Selection-Of-Articles-Vol-1.pdf

Kim, Taeyoung; Jeong, Suung; Lee, Julak (2022, March): Factors of Mass Casualty Terrorism. *Security Journal*, 35(1), 133-153. DOI: https://doi.org/10.1057/s41284-020-00268-w

Kim, Wukki; George, Justin; Sandler, Todd (2021, February-March): Introducing Transnational Terrorist Hostage Event (TTHE) Data Set, 1978 to 2018. *Journal of Conflict Resolution*, 65(2-3), 619-641. DOI: https://doi.org/10.1177/0022002720957714

Kirsch, Thomas D. et al. (2022, July-August): Opportunities to Strengthen the National Disaster Medical System: The Military–Civilian NDMS Interoperability Study. *Health Security,* 20(4), 339-347. DOI: https://doi.org/10.1089/hs.2021.0221

Klenka, Michal (2019, June): Major Incidents that Shaped Aviation Security. *Journal of Transportation Security*, 12(1), 39-56. DOI: https://doi.org/10.1007/s12198-019-00201-2

Klenka, Michal (2021, December): Aviation Cyber Security: Legal Aspects of Cyber Threats. *Journal of Transportation Security*, 14(3-4), 177-195. DOI: https://doi.org/10.1007/s12198-021-00232-8

Kooi, Brandon (2015): Security Concerns at Hot-Spot Bus Stop Locations. *Journal of Applied Security Research*, 10(3), 277-307. DOI: https://doi.org/10.1080/19361610.2015.1038762

Komasová, Sarah (2020): Airport Security and Visibility: Security as Visualization and its In-Place Performance. *Journal of Applied Security Research*, 15(3), 332-354. DOI: https://doi.org/10.1080/19361610.2020.1738315

Kostyuchenko, Yuriy V. et al. (2020): On the Behavior-Based Risk Communication Models in Crisis Management and Social Risks Minimization. *International Journal of Cyber Warfare and Terrorism*, 10(2), 27-45. DOI: https://doi.org/10.4018/IJCWT.2020040102

Kumar, Venkatachary Sampath; Prasad, Jagdish; Samikannu, Ravi (2018, May): A Critical Review of Cyber Security and Cyber Terrorism – Threats to Critical Infrastructure in the Energy Sector. *International Journal of Critical Infrastructures*, 14(2), 101-119. DOI: https://doi.org/10.1504/IJCIS.2018.091932

Labaj, Leo; Barnes, Bruce (2016, Spring): Protecting the Power Grid: Target Analysis and Vulnerability Assessment. *Journal of Counterterrorism & Homeland Security International*, 22(1), 26-28. URL: https://issuu.com/fusteros/docs/iacsp_magazine_v22_n1_issuu

Lee, Chia-yi (2022, May): Why do Terrorists Target the Energy Industry? A Review of Kidnapping, Violence and Attacks Against Energy Infrastructure. *Energy Research & Social Science*, 87, Article 102459. DOI: https://doi.org/10.1016/j.erss.2021.102459

Le Sage, Tanya; Borrion, Hervé; Toubaline, Sonia (2014, December): A User-Layered Approach for Modelling and Simulating Terrorist Attacks. *International Journal of Critical Infrastructures*, 10(3-4), 398-412. DOI: https://doi.org/10.1504/IJCIS.2014.066342 URL: https://discovery.ucl.ac.uk/id/eprint/1401091

Li, Chenglong (2021): Optimization of Emergency Resource Scheduling in Serial Terrorist Attacks Based on PSO-CS Algorithm. *Journal of Applied Security Research*, 16(4), 526-537. DOI: https://doi.org/10.1080/19361610.2020.1812995

Li, Shuying; Zhuang, Jun; Shen, Shifei (2017, June): A Three-Stage Evacuation Decision-Making and Behavior Model for the Onset of an Attack. *Transportation Research Part C: Emerging Technologies*, 79, 119-135. DOI: https://doi.org/10.1016/j.trc.2017.03.008 URL: https://www.eng.buffalo.edu/~jzhuang/Papers/LZS_TRC_2017.pdf

Liedlbauer, Lina (2021): Politicising European Counter-Terrorism: The Role of NGOs. *European Security*, 30(3), 485-503. DOI: https://doi.org/10.1080/09662839.2021.1947802

Liscouski, Robert; McGann, William (2016, May): The Evolving Challenges for Explosive Detection in the Aviation Sector and Beyond. *CTC Sentinel*, 9(5), 1-6. URL: https://ctc.westpoint.edu/wp-content/uploads/2016/05/CTC-SENTINEL_Vol9Iss515.pdf

Liu, Brooke Fisher; Fraustino, Julia Daisy (2014, September): Beyond Image Repair: Suggestions for Crisis Communication Theory Development. *Public Relations Review,* 40(3), 543-546. DOI: https://doi.org/10.1016/j.pubrev.2014.04.004

Liu, Brooke Fisher; Jin, Yan; Austin, Lucinda (2023): Digital Crisis Communication Theory: Current Landscape and Future Trajectories. In: Carl H. Botan; Erich J. Sommerfeldt (Eds.): *Public Relations Theory III: In the Age of Publics*. (Routledge Communication Series). New York: Routledge, 191-212.

Liu, Brooke Fisher; Viens, Jeannette (2020): Crisis and Risk Communication Scholarship of the Future: Reflections on Research Gaps. *Journal of International Crisis and Risk Communication Research*, 3(1), 7-14. URL: https://jicrcr.com/index.php/jicrcr/article/download/27/28/55

Liu, Brooke Fisher et al. (2017, April): Public Understanding of Medical Countermeasures. *Health Security*, 15(2), 137-143. DOI: https://doi.org/10.1089/hs.2016.0074

Liu, Brooke Fisher et al. (2017, October): The Role of Communication in Healthcare Systems and Community Resilience. *International Journal of Emergency Management*, 13(4), 305-327. DOI: https://doi.org/10.1504/IJEM.2017.087218

Liu, Brooke Fisher et al. (2018, November): Keeping Hospitals Operating During Disasters Through Crisis Communication Preparedness. *Public Relations Review*, 44(4), 585-597. DOI: https://doi.org/10.1016/j.pubrev.2018.06.002

Loadenthal, Michael (2015): Shooting Yourself in the Foot: Securitization, Critical Infrastructure, and the Gaza Strip. *Journal of Applied Security Research,* 10(2), 267-276. DOI: https://doi.org/10.1080/19361610.2015.1004607

Loadenthal, Michael (2022): Feral Fascists and Deep Green Guerrillas: Infrastructural Attack and Accelerationist Terror. *Critical Studies on Terrorism*, 15(1), 169-208. DOI: https://doi.org/10.1080/17539153.2022.2031129

Loffi, Jon M.; Bliss, Timm J.; Depperschmidt, Chad L. (2013, September): Identifying Knowledge Demands and Professional Skill Sets for Employment Within the Aviation Security Environment: A Qualitative Inquiry of Aviation Security Professionals. *Journal of Transportation Security*, 6(3), 235-256. DOI: https://doi.org/10.1007/s12198-013-0114-2

Lohlker, Rüdiger (2013): Al-Qaeda Airlines: Jihadi Self-Assessment and the Ideology of Engineers. In: Rüdiger Lohlker; Tamara Abu-Hamdeh (Eds.): *Jihadi Thought and Ideology*. (Jihadism and Terrorism, Vol. 1). Berlin: Logos, 5-15. URL: http://www.academia.edu/4396804/Al_Qaeda_Airlines

Lowe, David (2015): The Threat Islamist Groups Pose to the Security of European Union Member States: Time to Consider Re-Introducing the EU's Directive on the Use of Passenger Name Record Data. *International Journal of Terrorism and Political Hot Spots*, 10(3), 77-94.

Lowe, Luis et al. (2020, September): Geospatial Analysis in Responding to a Nuclear Detonation Scenario in NYC: The Gotham Shield Exercise. *Journal of Homeland Security and Emergency Management*, 17(3), Article 20190027. DOI: https://doi.org/10.1515/jhsem-2019-0027

Lum, Cynthia et al. (2015, October): Discretion and Fairness in Airport Security Screening. *Security Journal*, 28(4), 352-373. DOI: https://doi.org/10.1057/sj.2012.51

Lyovin, Boris A. et al. (2019, September): Method for Remote Rapid Response to Transportation Security Threats on High Speed Rail Systems. *International Journal of Critical Infrastructures*, 15(4), 324-335. DOI: https://doi.org/10.1504/IJCIS.2019.103015

Maclachlan, Colin (2016): The Threat of Terrorism to Critical Infrastructure: TEN-R and the Global Salafi Jihad. In: Scott Nicholas Romaniuk; Stewart Tristan Webb (Eds.): *Insurgency and Counterinsurgency in Modern War*. Boca Raton: CRC Press, 89-106.

Malet, David; Korbitz, Mark (2015, November): Bioterrorism and Local Agency Preparedness: Results from an Experimental Study in Risk Communication. *Journal of Homeland Security and Emergency Management,* 12(4), 861-873. DOI: https://doi.org/10.1515/jhsem-2014-0107

Manning, Scott Robert (2020, September): Strategic Planning in Emergency Management: Evaluating the Impacts on Local Program Quality. *Journal of Homeland Security and Emergency Management*, 17(3), Article 20190051. DOI: https://doi.org/10.1515/jhsem-2019-0051

Maras, Marie-Helen (2014): Critical Infrastructure Protection. In: *The CRC Press Terrorism Reader*. Boca Raton: CRC Press, 291-306.

Marino, Michael et al. (2015, June): To Save Lives and Property: High Threat Response. *Homeland Security Affairs,* 11, Article 5. DOI: https://www.hsaj.org/articles/4530

Marjanian, Ali; Soleymani, Soodabeh (2018, January): Optimal Investment in Power System for Defending Against Malicious Attacks Through Defender-Attacker-Defender Model and Mixed Strategy Nash Equilibrium. *International Journal of Critical Infrastructures*, 13(4), 354-373. DOI: https://doi.org/10.1504/IJCIS.2017.089242

Marshall, Zachary A. et al. (2022, December): Expediting Airport Security Queues Through Advanced Lane Assignment. *Journal of Transportation Security,* 15(3-4), 245-262. DOI: https://doi.org/10.1007/s12198-022-00247-9

Martinez, DeAndrea et al. (2019, November-December): Evolution of the Public Health Preparedness and Response Capability Standards to Support Public Health Emergency Management Practices and Processes. *Health Security*, 17(6), 430-438. DOI: https://doi.org/10.1089/hs.2019.0076

Maiello, Mark L.; Mandel-Ricci, Jenna (2024, November-December): Findings and Recommendations from a Series of Workshops on Hospital Emergency Responses to an Improvised Nuclear Device Detonation. *Health Security*, 22(6), 409-421. DOI: https://doi.org/10.1089/hs.2023.0106

McCarthy, John; Mahoney, William (2013): SCADA Threats in the Modern Airport. *International Journal of Cyber Warfare and Terrorism*, 3(4), 32-39. DOI: https://doi.org/10.4018/ijcwt.2013100104

McCormack, Desmond; Horner, William; Smith, Jerry (2017, March): On-Site Risk Surveys with an Aligned Approach for Physical and Cyber Security to Reduce the Potential Exposure from Cyber-Attacks on Industrial Control Systems. *The Journal of Terrorism & Cyber Insurance*, 1(2), 25-33. URL: http://docs.wixstatic.com/ugd/7cfaab_dbd9c13d3c3d42049cf078a3e876b28a.pdf

McCourt, Alexander D.; Sunshine, Gregory; Rutkow, Lainie (2019, May-June): Judicial Opinions Arising from Emergency Preparedness, Response, and Recovery Activities. *Health Security*, 17(3), 240-247. DOI: https://doi.org/10.1089/hs.2018.0118

McCreight, Robert (2019): Grid Collapse Security, Stability and Vulnerability Issues: Impactful Issues Affecting Nuclear Power Plants, Chemical Plants and Natural Gas Supply Systems. *Journal of Homeland Security and Emergency Management*, 16(1), Article 20180021. DOI: https://doi.org/10.1515/jhsem-2018-0021

McCrie, Robert; Haas, David (2018): Why Airline Passenger Screening Will Be With Us Forever: Past, Present, and Prospects for Air Travel Safety. *Journal of Applied Security Research*, 13(2), 149-159. DOI: https://doi.org/10.1080/19361610.2018.1422359

McFarlane, Paul (2023, December): A New Inter-Disciplinary Relationship: Introducing Self-Organized Criticality to Failures in Aviation Security. *Journal of Transportation Security,* 16(1), Article 12. DOI: https://doi.org/10.1007/s12198-023-00257-1

Mendizabal, Agustin Palao et al. (2022, September): Using Hotspot Analysis to Prioritize Security Efforts in Colombian Critical Infrastructure, a Focus on the Power Grid. *Security Journal*, 35(3), 801-822. DOI: https://doi.org/10.1057/s41284-021-00300-7

Mezher, Toufic; El Khatib, Sameh; Sooriyaarachchi, Thilanka Maduwanthi (2015): Cyberattacks on Critical Infrastructure and Potential Sustainable Development Impacts. *International Journal of Cyber Warfare and Terrorism*, 5(3), 1-18. DOI: https://doi.org/10.4018/IJCWT.2015070101

Miller, Jacob et al. (2024, December): Multi-Layer Network PageRank for Critical Infrastructure Analysis. *Homeland Security Affairs*, 20(4). URL: https://www.hsaj.org/articles/23189

Milioti, Christina et al. (2019, December): Modeling Traveler Recovery Time Following Man-Made Incidents: The Case of the Athens Metro. *Journal of Transportation Security*, 12(3-4), 103-117. DOI: https://doi.org/10.1007/s12198-019-00205-y

Mitchener-Nissen, Timothy; Bowers, Kate; Chetty, Kevin (2012, July): Public Attitudes to Airport Security: The Case of Whole Body Scanners. *Security Journal*, 25(3), 229-243. DOI: https://doi.org/10.1057/sj.2011.20

Monaghan, Aidan (2017, May): Implications of September 11 Flight Transponder Activity. *Journal of 9/11 Studies*. URL: http://www.journalof911studies.com/implications-of-september-11-flight-transponder-activity

Morabito, Patrick N. et al. (2011, November-December): Impact of Personal Communication Networks on Emergency Evacuation Times. *Journal of Emergency Management*, 9(6), 75-80. DOI: https://doi.org/10.5055/jem.2011.0081

Myers, Natalie et al. (2016, August): People, Infrastructure, and Conflict: Analyzing the Dynamics of Infrastructure Disruption and Community Response. *Small Wars Journal.* URL: https://archive.smallwarsjournal.com/jrnl/art/people-infrastructure-and-conflict-analyzing-the-dynamics-of-infrastructure-disruption-and-

Myers, Nathan (2020, May): Coordination, Communication, and Clade X: Challenges and Lessons Learned from Health Emergency Exercise After-Action Reports and How They Can Help Guide Future Efforts to Improve Information Sharing. *Journal of Homeland Security and Emergency*

*Management*, 17(2), Article 20180048. DOI: https://doi.org/10.1515/jhsem-2018-0048

Narloch, Andrew (2019, July): COIN Primer – The MANPADS Republic: An Effective Means to Establish Regional Sovereignty. *Small Wars Journal*. URL: https://archive.smallwarsjournal.com/index.php/jrnl/art/coin-primer-manpads-republic-effective-means-establish-regional-sovereignty

Niglia, Alessandro; Torretta, Letizia (2017): Preventing Terroristic Attacks Against Cultural Heritage as Part of a Critical Infrastructure Protection Strategy. In: Alessandro Niglia; Amer Al Sabaileh; Amani (Amneh) Hammad (Eds.): *Countering Terrorism, Preventing Radicalization and Protecting Cultural Heritage: The Role of Human Factors and Technology.* (NATO Science for Peace and Security Series – E: Human and Societal Dynamics, Vol. 133). Amsterdam: IOS Press, 1-16.

Nøkleberg, Martin (2022, April): Expecting the Exceptional in the Everyday: Policing Global Transportation Hubs. *Security Dialogue*, 53(2), 164-181. DOI: https://doi.org/10.1177/09670106211007066

Norri-Sederholm, Teija; Huhtinen, Aki-Mauri; Paakkonen, Heikki (2018): Ensuring Public Safety Organisations' Information Flow and Situation Picture in Hybrid Environments. *International Journal of Cyber Warfare and Terrorism*, 8(1), 12-24. DOI: https://doi.org/10.4018/IJCWT.2018010102

Olmati, Pierluigi et al. (2015, October): Blast Resistant Design of Precast Reinforced Concrete Walls for Strategic Infrastructures Under Uncertainty. *International Journal of Critical Infrastructures*, 11(3), 197-212. DOI: https://doi.org/10.1504/IJCIS.2015.072151

Pala, Ali; Zhuang, Jun (2018, March): Security Screening Queues with Impatient Applicants: A New Model with a Case Study. *European Journal of Operational Research*, 265(3), 919-930. DOI: https://doi.org/10.1016/j.ejor.2017.08.038

Parrott, Michael W. (2024, April): Weaponizing Food Insecurity: The Violent Extremist Threat to Precision Agriculture in the United States. In: Susan Sim; Eric Hartunian; Paul J. Milas (Eds.): *Emerging Technologies and Terrorism: An American Perspective*. Carlisle: US Army War College Press, 35-51. URL: https://press.armywarcollege.edu/monographs/967

Pastorello, Mauro (2015): How Cyberspace is Used by Terrorist Organization: Possible Threats to Critical Infrastructures? The Most Recent Activities of Cyber Counterterrorism. *Sicurezza, Terrorismo e Società*, 2, 117-134. URL: http://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2015/12/Pastorello_SicTerSoc_book-8.pdf

Patil, Sunil et al. (2014): Trade-off Across Privacy, Security and Surveillance in the Case of Metro Travel in Europe. *Transportation Research Procedia*, 1(1), 121-132. DOI: https://doi.org/10.1016/j.trpro.2014.07.013

Pearce, Julia M. et al. (2013): Communicating with the Public Following Radiological Terrorism: Results from a Series of Focus Groups and National Surveys in Britain and Germany. *Prehospital and Disaster Medicine*, 28(2), 110-119. DOI: https://doi.org/10.1017/S1049023X12001756

Perry, Gali; Hasisi, Badi (2020): Closing the Gap: Promoting Suspect Communities' Cooperation with Airport Security. *Terrorism and Political Violence*, 32(6), 1141-1160. DOI: https://doi.org/10.1080/09546553.2018.1442331

Peter, Cyril (2016): Cruising with Terrorists: Qualitative Study of Consumer Perspectives. *International Journal of Safety and Security in Tourism/Hospitality*, 14. URL: https://www.palermo.edu/Archivos_content/2016/Economicas/journal-tourism/edicion14/01_CruisingWithTerrorists.pdf

Petersen, Laura et al. (2023, December): Applicability of PROACTIVE Recommendations on CBRNe Risks and Threats to Passenger Rail and Metro Sectors. *Journal of Transportation Security*, 16(1), Article 4. DOI: https://doi.org/10.1007/s12198-023-00263-3

Phayal, Anup et al. (2024, June): Attrition and Provocation: Subnational Variation in Terrorist Targeting. *Perspectives on Terrorism*, 18(2), 57-81. URL: https://pt.icct.nl/sites/default/files/2024-06/Research%20article_Zhang.pdf

Pik, Eugene (2024, December): Airport Security: The Impact of AI on Safety, Efficiency, and the Passenger Experience. *Journal of Transportation Security*, 17(1), Article 9. DOI: https://doi.org/10.1007/s12198-024-00276-6

Pousette, Anders et al. (2021, June): AERODROM Security Climate: Development and Validation of the Aerodrome Security Climate Questionnaire (ADSECQ). *Journal of Transportation Security*, 14(1-2), 19-39. DOI: https://doi.org/10.1007/s12198-020-00217-z

Pretorius, Barend; van Niekerk, Brett (2016): Cyber-Security for ICS/SCADA: A South African Perspective. *International Journal of Cyber Warfare and Terrorism*, 6(3), 1-16. DOI: https://doi.org/10.4018/IJCWT.2016070101

Prunckun, Henry; Whitford, Troy (2019): Protection of Critical Infrastructure. In: *Terrorism and Counterterrorism: A Comprehensive Introduction to Actors and Actions.* Boulder: Lynne Rienner, 191-210.

Quashie, Emanuel Patrick (2023, September): The War on Terror and the Caribbean. *Perspectives on Terrorism*, 17(3), 70-82. URL: https://pt.icct.nl/sites/default/files/2023-09/PT%20-%20Vol%20XVII%2C%20Issue%20III%20-%20Quashie.pdf

Radomyski, Adam; Bernat, Paweł (2018): Contemporary Determinants of Organising Effective Protection of Civil Aviation Against Terrorism. *Transportation Research Procedia*, 35, 259-270. DOI: https://doi.org/10.1016/j.trpro.2018.12.021

Richman, Ety (2015): The Need for Integrated Municipal Planning for Rail Security the Jerusalem Light Rail Project. In: Aaron Richman; Yair Sharan (Eds.): *Lone Actors – An Emerging Security Threat*. (NATO Science for Peace and Security Series – E: Human and Societal Dynamics, Vol. 123). Amsterdam: IOS Press, 221-232.

Riedman, David (2016, May): Questioning the Criticality of Critical Infrastructure: A Case Study Analysis. *Homeland Security Affairs*, 12, Essay 3. DOI: https://www.hsaj.org/articles/10578

Riedman, David (2017, June): The Cold War on Terrorism: Reevaluating Critical Infrastructure Facilities as Targets for Terrorist Attacks. *Homeland Security Affairs*, 13, Article 3. URL: https://www.hsaj.org/articles/13976

Riley, K. Jack (2011): Flight of Fancy? Air Passenger Security Since 9/11. In: Brian Michael Jenkins; John P. Godges (Eds.) (2011): *The Long Shadow of 9/11: America's Response to Terrorism*. [e-Book]. (RAND Monographs, MG-1107-RC). Santa Monica: RAND Corporation, 147-160. DOI: https://doi.org/10.7249/MG1107

Ríos, Jerónimo; González, Julio C.; García de las Heras, Mariano (2023): Environment and Armed Conflict in Colombia: Terrorist Attacks Against Water Resources and Oil Infrastructure in Norte de Santander (2010-2020). *Small Wars & Insurgencies*, 34(8), 1429-1457. DOI: https://doi.org/10.1080/09592318.2021.1978750

Rooijakkers, Maria; Sadiq, Abdul-Akeem (2015, April): Critical Infrastructure, Terrorism, and the Chemical Facility Anti-Terrorism Standards: The Need for Collaboration. *International Journal of Critical Infrastructures*, 11(2), 167-182. DOI: https://doi.org/10.1504/IJCIS.2015.068615

Rosbough, Christopher P. (2012): Property Crime at the Atlanta International Airport: An Examination of the Rational Choice Theory and the 9/11 Intervention. *Journal of Applied Security Research*, 7(3), 354-374. DOI: https://doi.org/10.1080/19361610.2012.686097

Rose, Adam Z.; Avetisyan, Misak; Chatterjee, Samrat (2014, August): A Framework for Analyzing the Economic Tradeoffs Between Urban Commerce and Security Against Terrorism. *Risk Analysis*, 34(8), 1554-1579. DOI: https://doi.org/10.1111/risa.12187

Rosoff, Heather et al. (2012, September): Structuring Uncertainty and Conflicting Objectives for Life or Death Decisions Following an Urban Biological Catastrophe. *IDRiM Journal*, 2(1), 49-69. DOI: https://doi.org/10.5595/idrim.2012.0035

Rosson, Jack et al. (2019, May): Incentivizing Cyber Security Investment in the Power Sector Using an Extended Cyber Insurance Framework. *Homeland Security Affairs*, 15, Article 2. URL: https://www.hsaj.org/articles/15082

Rudner, Martin (2013): Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge. *International Journal of Intelligence and CounterIntelligence*, 26(3), 453-481. DOI: https://doi.org/10.1080/08850607.2013.780552

Russell, Jill S.; de Orellana, Pablo (2020): Public Communications Leadership: #CrisisComms and the Manchester Arena Attack. *The RUSI Journal*, 165(5-6), 22-35. DOI: https://doi.org/10.1080/03071847.2020.1845099

Salehian, Ali; Sheikholeslami, Mohammad Hasan (2022): The Impact of the Aviation Industry on International Security Threats, Case Study of Health Threats (2002–2020). *Journal of Applied Security Research*, 17(4), 477-496. DOI: https://doi.org/10.1080/19361610.2021.1896280

Sarhadi, Hassan; Tulett, David M.; Verma, Manish (2017, March): An Analytical Approach to the Protection Planning of a Rail Intermodal Terminal Network. *European Journal of Operational Research*, 257(2), 511-525. DOI: https://doi.org/10.1016/j.ejor.2016.07.036

Satish, Ajay Sudharshan; Mangal, Akul; Churi, Prathamesh (2023, December): A Systematic Review of Passenger Profiling in Airport Security System: Taking a Potential Case Study of CAPPS II. *Journal of Transportation Security*, 16(1), Article 8. DOI: https://doi.org/10.1007/s12198-023-00260-6

Schlegelmilch, Jeffrey et al. (2017, Spring): Acts of Terrorism and Mass Violence Targeting Schools: Analysis and Implications for Preparedness in the USA. *Journal of Business Continuity & Emergency Planning*, 10(3), 280-289. DOI: https://doi.org/10.7916/D84X5DH5

Schouten, Peer (2014): Security as Controversy: Reassembling Security at Amsterdam Airport. *Security Dialogue*, 45(1), 23-42. DOI: https://doi.org/10.1177/0967010613515014

Seasonwein, Robert (2016, Spring): The Challenge of Passenger Rail Security. *Journal of Counterterrorism and Homeland Security International*, 22(1), 12-13. URL: https://issuu.com/fusteros/docs/iacsp_magazine_v22_n1_issuu

Seeger, Matthew W. et al. (2018, May-June): A Conceptual Model for Evaluating Emergency Risk Communication in Public Health. *Health Security*, 16(3), 193-203. DOI: https://doi.org/10.1089/hs.2018.0020

Senthil, K.; Sethi, Muskaan; Pelecanos, Loizos (2023, June): Techniques to Safeguard the Underground Tunnels Against Surface Blast Load. *International Journal of Critical Infrastructures*, 19(4), 301-322. DOI: https://doi.org/10.1504/IJCIS.2023.132212

Shi, Jia et al. (2017, April): Assessing Risk Communication in Social Media for Crisis Prevention: A Social Network Analysis of Microblog. *Journal of Homeland Security and Emergency Management*, 14(1), Article 20160058. DOI: https://doi.org/10.1515/jhsem-2016-0058

Siao, Daniel H. (2017, April): The Aviation Insider Threat: An Assessment of Vulnerabilities and Countermeasures. *Harvard National Security Journal,* Online Edition. URL: https://harvardnsj.org/2017/04/24/the-aviation-insider-threat-an-assessment-of-vulnerabilities-and-countermeasures

Sinai, Joshua (2012, Fall): New Trends in Airport and Aviation Security. *Journal of Counterterrorism and Homeland Security International*, 18(3), 18-27. URL: https://issuu.com/fusteros/docs/iacsp_magazine_v18n3

Sinai, Joshua (2017, Winter): Active Threats Against the Aviation Sector: Terrorism, Active Shooters, Workplace Violence, and "Insiders". *Journal of Counterterrorism and Homeland Security International*, 22(4), 32-37. URL: https://issuu.com/fusteros/docs/iacsp_magazine_v22n4_issuu

Sjoberg, Laura (2015, April): (S)he Shall Not Be Moved: Gender, Bodies and Travel Rights in the Post-9/11 Era. *Security Journal*, 28(2), 198-215. DOI: https://doi.org/10.1057/sj.2015.4

Smith, Patrick K. et al. (2014, March): Network-Based Risk Assessment of the US Crude Pipeline Infrastructure. *International Journal of Critical Infrastructures*, 10(1), 67-80. DOI: https://doi.org/10.1504/IJCIS.2014.059550

Song, Cen; Zhuang, Jun (2017, September): N-Stage Security Screening Strategies in the Face of Strategic Applicants. *Reliability Engineering & System Safety*, 165, 292-301. DOI: https://doi.org/10.1016/j.ress.2017.04.019

Spyridopoulos, Theodoros et al. (2017): Critical Infrastructure Cyber-Security Risk Management. In: Maura Conway et al. (Eds.): *Terrorists' Use of the Internet*. (NATO Science for Peace and Security Series – E: Human and Societal Dynamics, Vol. 136). Amsterdam: IOS Press, 59-76. DOI: https://doi.org/10.3233/978-1-61499-765-8-59

Stern, Eric K. (2017, June): Unpacking and Exploring the Relationship Between Crisis Management and Social Media in the Era of "Smart Devices". *Homeland Security Affairs*, 13, Article 4. DOI: https://www.hsaj.org/articles/13986

Stewart, Mark G.; Mueller, John (2013, May): Terrorism Risks and Cost-Benefit Analysis of Aviation Security. *Risk Analysis*, 33(5), 893-908. DOI: https://doi.org/10.1111/j.1539-6924.2012.01905.x URL: https://politicalscience.osu.edu/faculty/jmueller/FAMSraFIN.pdf

Stewart, Mark G.; Mueller, John (2014): A Risk and Cost–Benefit Analysis of Police Counter-Terrorism Operations at Australian Airports. *Journal of Policing, Intelligence and Counter Terrorism*, 9(2), 98-116. DOI: https://doi.org/10.1080/18335330.2014.940816 URL: https://politicalscience.osu.edu/faculty/jmueller/JPICT_AFP%202014fin.pdf

Stewart, Mark G.; Mueller, John (2014, March): Cost-Benefit Analysis of Airport Security: Are Airports too Safe? *Journal of Air Transport Management*, 35, 19-28. DOI: https://doi.org/10.1016/j.jairtraman.2013.11.003 URL: https://www.cato.org/sites/cato.org/files/articles/stewart-mueller-joatm.pdf

Stewart, Mark G.; Mueller, John (2017, June): Risk and Economic Assessment of Expedited Passenger Screening and TSA PreCheck. *Journal of Transportation Security*, 10(1-2), 1-22. DOI: https://doi.org/10.1007/s12198-016-0175-0 URL: https://politicalscience.osu.edu/faculty/jmueller/jtsfin.pdf

Stoichev, Kiril (2014): Security Levels of Critical Infrastructure. *Journal of Applied Security Research*, 9(3), 328-337. DOI: https://doi.org/10.1080/19361610.2014.913233

Stoichev, Kiril (2015): Selection of an Alternative Method for Establishing Security Levels. *Journal of Applied Security Research,* 10(1), 48-59. DOI: https://doi.org/10.1080/19361610.2015.972269

Stone, Kahler W. et al. (2018, December): Evaluating the Effectiveness of a Full-Scale Exercise of Epidemiologic Capacity for Bioterrorism Response. *Journal of Homeland Security and Emergency Management*, 15(4), Article 20170061. DOI: https://doi.org/10.1515/jhsem-2017-0061

Strandberg, Veronica (2013, September): Rail Bound Traffic—A Prime Target for Contemporary Terrorist Attacks? *Journal of Transportation Security*, 6(3), 271-286. DOI: https://doi.org/10.1007/s12198-013-0116-0

Strandh, Veronica (2017, December): Exploring Vulnerabilities in Preparedness – Rail Bound Traffic and Terrorist Attacks. *Journal of Transportation Security*, 10(3-4), 45-62. DOI: https://doi.org/10.1007/s12198-017-0178-5

Straub, Frank; Zeunik, Jennifer; Gorban, Ben (2017, May): Lessons Learned from the Police Response to the San Bernardino and Orlando Terrorist Attacks. *CTC Sentinel*, 10(5), 1-7. URL: https://ctc.westpoint.edu/wp-content/uploads/2017/05/CTC-Sentinel_Vol10Iss515.pdf

Suda, Yuko (2013, July): Transatlantic Politics of Data Transfer: Extraterritoriality, Counter-Extraterritoriality and Counter-Terrorism. *JCMS: Journal of Common Market Studies*, 51(4), 772-788. DOI: https://doi.org/10.1111/jcms.12017

Swain, Steve (2015): Securing the Transport System. In: Genevieve Lennon; Clive Walker (Eds.): *Routledge Handbook of Law and Terrorism*. (Routledge Handbooks). Abingdon: Routledge, 349-364.

Szyliowicz, Joseph S. (2013): Transportation Technology and Its Effect on the Speed, Distance and Magnitude of Terrorist Attacks. In: U. Feyyaz Aydoğdu (Ed.): *Technological Dimensions of Defence Against Terrorism.* (NATO Science for Peace and Security Series – E: Human and Societal Dynamics, Vol. 115). Amsterdam: IOS Press, 70-80. DOI: https://doi.org/10.3233/978-1-61499-317-9-70

Szymankiewicz, Łukasz (2022): Evolution of Aviation Terrorism – El Al Israeli Airlines, Case Study. *Journal of Strategic Security*, 15(1), 106-125. DOI: https://doi.org/10.5038/1944-0472.15.1.1945

Tabansky, L. (2013): Critical Infrastructure Protection: Evolution of Israeli Policy. *International Journal of Cyber Warfare and Terrorism*, 3(3), 80-87. DOI: https://doi.org/10.4018/ijcwt.2013070106

Tallis, Joshua; Bauer, Ryan; Frey, Lauren (2017, October): ISIL's Battlefield Tactics and the Implications for Homeland Security and Preparedness. *Journal of Terrorism Research*, 8(3), 24-42. DOI: https://doi.org/10.15664/jtr.1391

Tan, Jethro; Wang, Yingmin; Gomes, Danielle (2016): Building National Resilience in the Digital Era of Violent Extremism: Systems and People. In: Majeed Khader et al. (Eds.): *Combating Violent Extremism and Radicalization in the Digital Era*. Hershey: IGI Global, 307-327.

Taquechel, Eric (2013, September): Options and Challenges of a Resilience-Based, Network-Focused Port Security Grant Program. *Journal of Homeland Security and Emergency Management,* 10(2), 521-554. DOI: https://doi.org/10.1515/jhsem-2013-0018

Taquechel, Eric F.; Lewis, Ted G. (2016, September): More Options for Quantifying Deterrence and Reducing Critical Infrastructure Risk: Cognitive Biases. *Homeland Security Affairs*, 12, Article 3. URL: https://www.hsaj.org/articles/12007

Taquechel, Eric F.; Lewis, Ted G. (2017, October): A Right-Brained Approach to Critical

Infrastructure Protection Theory in Support of Strategy and Education: Deterrence, Networks, Resilience, and "Antifragility". *Homeland Security Affairs*, 13, Article 8. URL: https://www.hsaj.org/articles/14087

Taquechel, Eric F.; Saitgalina, Marina (2018, December): Risk-Based Performance Metrics for Critical Infrastructure Protection? A Framework for Research and Analysis. *Homeland Security Affairs*, 14, Article 8. URL: https://www.hsaj.org/articles/14699

TariVerdi, Mersedeh; Miller-Hooks, Elise; Kirsch, Thomas (2018, December): Strategies for Improved Hospital Response to Mass Casualty Incidents. *Disaster Medicine and Public Health Preparedness*, 12(6), 778-790. DOI: https://doi.org/10.1017/dmp.2018.4

Taylor, Robert W.; Swanson, Charles R. (2019): Emergency Management. In: *Terrorism, Intelligence, and Homeland Security*. (2nd ed.). New York: Pearson Education, 355-386.

Tennant, Denise L.; Nolan, Louis; House, Deanna (2024, Summer): Cyber Red Lines: Government Responses to Cyberattacks on Critical Infrastructure. Æther: *A Journal of Strategic Airpower & Spacepower,* 3(2), 59-71. URL: https://www.airuniversity.af.edu/Portals/10/AEtherJournal/Journals/Volume-3_Number-2/Aether_Volume_3_Number_2.pdf

Thornton, Richard C. (2013): The Hijacking of TWA-847: A Strategic Analysis. In: Jussi M. Hanhimäki; Bernhard Blumenau (Eds.): *An International History of Terrorism: Western and Non-Western Experiences*. (Political Violence). Abingdon: Routledge, 133-148.

Tichý, Lukáš (2019, June): Energy Infrastructure as a Target of Terrorist Attacks from the Islamic State in Iraq and Syria. *International Journal of Critical Infrastructure Protection*, 25, 1-13. DOI: https://doi.org/10.1016/j.ijcip.2019.01.003

Tichý, Lukáš; Eichler, Jan (2018): Terrorist Attacks on the Energy Sector: The Case of Al Qaeda and the Islamic State. *Studies in Conflict & Terrorism*, 41(6), 450-473. DOI: https://doi.org/10.1080/1057610X.2017.1323469

Tripathi, Kartikeya; Borrion, Hervé (2016, February): Safe, Secure or Punctual? A Simulator Study of Train Driver Response to Reports of Explosives on a Metro Train. *Security Journal*, 29(1), 87-105. DOI: https://doi.org/10.1057/sj.2015.46

Turner, James Austin et al. (2020, July-August): Willingness to Respond to Radiological Disasters Among First Responders in St. Louis, Missouri. *Health Security,* 18(4), 318-328. DOI: https://doi.org/10.1089/hs.2019.0160

Turner, James Austin et al. (2020, September): First Responders' and Librarians' Intention to Use Web-Based Resources for Response Information During Biological, Chemical, and Radiological Terrorism Events. *Journal of Homeland Security and Emergency Management,* 17(3), Article 20190030. DOI: https://doi.org/10.1515/jhsem-2019-0030

Turtz, Michael (2024, December): Comparative Policy Analysis in Airport Security Through the Lenses of the Multiple-Streams Framework. *Journal of Transportation Security*, 17(1), Article 15. DOI: https://doi.org/10.1007/s12198-024-00284-6

Tziarras, Zenonas (2017): Islamic Caliphate: A Quasi-State, a Global Security Threat. *Journal of Applied Security Research*, 12(1), 96-116. DOI: https://doi.org/10.1080/19361610.2017.1228038

Unlu, Ali et al. (2012): The Impact of 9/11 on Information Policy in the United States: A Current Perspective on Homeland Security and Emergency Management. *Journal of Applied Security Research*, 7(3), 320-340. DOI: https://doi.org/10.1080/19361610.2012.686095

Valkenburg, Govert; van der Ploeg, Irma (2015, August): Materialities Between Security and Privacy: A Constructivist Account of Airport Security Scanners. *Security Dialogue*, 46(4), 326-344. DOI: https://doi.org/10.1177/0967010615577855

van der Wal, C. Natalie et al. (2021, April): Evacuation Behaviors and Emergency Communications: An Analysis of Real-World Incident Videos. *Safety Science*, 136, Article 105121. DOI: https://doi.org/10.1016/j.ssci.2020.105121

Varouhakis, Myron; Stewart, Mark (2015, Winter): ISAF's Afghan Truck Drivers: The Overlooked Counterinsurgency Population. *Journal of Strategic Security*, 8(4), 92-113. DOI: https://doi.org/10.5038/1944-0472.8.4.1457

Veilleux, Jennifer; Dinar, Shlomi (2021): A Global Analysis of Water-Related Terrorism, 1970–2016. *Terrorism and Political Violence*, 33(6), 1191-1216. DOI: https://doi.org/10.1080/09546553.2019.1599863

Verner, Duane; Petit, Frederic; Kim, Kibaek (2017, October): Incorporating Prioritization in

Critical Infrastructure Security and Resilience Programs. *Homeland Security Affairs*, 13, Article 7. URL: https://www.hsaj.org/articles/14091

Vivek, Skanda; Harry, Charles (2022): Evaluating the Strategic Consequences of Cyber Targeting Strategies on Road Transport Networks: A Case Study of Washington DC. *International Journal of Cyber Warfare and Terrorism*, 12(1). DOI: https://doi.org/10.4018/IJCWT.314942

Vollmer, Maike et al. (2024, May): Standardization Gaps in European Disaster Management. *Journal of Homeland Security and Emergency Management*, 21(2), 209-242. DOI: https://doi.org/10.1515/jhsem-2021-0047

Vukadinovic, Danijela; Ruiz Osés, Miguel; Anderson, David (2023, December): Automated Detection of Inorganic Powders in X-Ray Images of Airport Luggage. *Journal of Transportation Security*, 16(1), Article 3. DOI: https://doi.org/10.1007/s12198-023-00261-5

Wahyudi, Rizki; Priyanto, Sapto (2022, May): Prevention of Terrorism Attacks Through Environmental Design in Indonesia Airport. *Journal of Terrorism Studies*, 4(1), Article 3. URL: https://scholarhub.ui.ac.id/jts/vol4/iss1/3

Wang, Bairong; Zhuang, Jun (2018, September): Rumor Response, Debunking Response, and Decision Makings of Misinformed Twitter Users During Disasters. *Natural Hazards*, 93(3), 1145-1162. DOI: https://doi.org/10.1007/s11069-018-3344-6

Wang, Chen; Bier, Vicki M. (2012, April): Optimal Defensive Allocations in the Face of Uncertain Terrorist Preferences, with an Emphasis on Transportation. *Homeland Security Affairs*, Suppl. 4, Article 4. URL: https://www.hsaj.org/articles/210

Wardin, Katarzyna (2020, December): Security of Passenger Transport in the Baltic Sea in the Context of Foreign Terrorist Fighters. *Journal of Transportation Security*, 13(3-4), 215-229. DOI: https://doi.org/10.1007/s12198-020-00213-3

Watkins, Daniel M. et al. (2015, September): Identifying Security Checkpoint Locations to Protect the Major U.S. Urban Areas. *Homeland Security Affairs*, 11, Article 8. URL: https://www.hsaj.org/articles/6311

Weiss, Jim; Davis, Mickey (2012, Spring): The Boeing 727 Anti Terrorism Training Facility. *Journal of Counterterrorism and Homeland Security International*, 18(1), 30-34. URL: https://issuu.com/fusteros/docs/iacsp_magazine_v18n1

Wendling, Cécile (2012): The Development of European Union Emergency and Crisis Management Structures. In: Christian Kaunert; Sarah Léonard; Patryk Pawlak (Eds.): *European Homeland Security: A European Strategy in the Making?* (Contemporary Security Studies). Abingdon: Routledge, 111-125.

West, Laura B. (2021, June): Building Cyber Walls: Executive Emergency Powers in Cyberspace. *Journal of National Security Law and Policy*, 11(3), 591-634. URL: https://jnslp.com/2021/06/02/building-cyber-walls-executive-emergency-powers-in-cyberspace

Westbrook, Tegg (2019): The Global Positioning System and Military Jamming: The Geographies of Electronic Warfare. *Journal of Strategic Security,* 12(2), Article 1. DOI: https://doi.org/10.5038/1944-0472.12.2.1720

Wetter, Olive Emil; Wüthrich, Valentino (2015): "What Is Dear to You?" Survey of Beliefs Regarding Protection of Critical Infrastructure Against Terrorism. *Defense & Security Analysis,* 31(3), 185-198. DOI: https://doi.org/10.1080/14751798.2015.1056941

White, Latechia; Eveleigh, Timothy; Bereket, Tanju (2019): A Hybrid Hierarchical Framework Toward Security Effectiveness for Critical Infrastructure Protection and Resiliency: A Hospital Case Study. *Journal of Homeland Security and Emergency Management,* 16(1), Article 20140111. DOI: https://doi.org/10.1515/jhsem-2014-0111

Wigginton, Michael, Jr. et al. (2014): What Is the Role of Behavioral Analysis in a Multilayered Approach to Aviation Security? *Journal of Applied Security Research*, 9(4), 393-417. DOI: https://doi.org/10.1080/19361610.2014.942828

Williams, Alex; Corner, Emily; Taylor, Helen (2022): Vehicular Ramming Attacks: Assessing the Effectiveness of Situational Crime Prevention Using Crime Script Analysis. *Terrorism and Political Violence*, 34(8), 1549-1563. DOI: https://doi.org/10.1080/09546553.2020.1810025

Wolbers, Jeroen (2022, December): Understanding Distributed Sensemaking in Crisis Management: The Case of the Utrecht Terrorist Attack. *Journal of Contingencies and Crisis Management*, 30(4), 401-411. DOI: https://doi.org/10.1111/1468-5973.12382

Wood, Michele M. et al. (2018, June): Milling and Public Warnings. *Environment and Behavior,* 50(5), 535-566. DOI: https://doi.org/10.1177/0013916517709561

Wood, Steve; Gardiner, Simon (2021): Policing U.K. Airports and Schedule 7 of the Terrorism Act 2000: The Young Passengers' Perception of Security Measures. *Terrorism and Political Violence*, 33(8), 1621-1642. DOI: https://doi.org/10.1080/09546553.2019.1638255

Wood, Steve; Raj, Razaq (2021, June): The Impact of Security Scanners at Airports and Ethnic Minority Travellers' Experience. *Security Journal*, 34(2), 278 -298. DOI: https://doi.org/10.1057/s41284-019-00222-5 URL: https://eprints.leedsbeckett.ac.uk/id/eprint/6338

Woods, Steve (2017): Terrorism in Aviation: Going on Holiday? Young Travellers Take Longer to Pass Through Security: Aviation, Security, Passenger Experience, Terrorism. *International Journal of Safety and Security in Tourism/Hospitality,* 16. URL: https://www.palermo.edu/Archivos_content/2017/Economicas/journal-tourism/edicion16/PAPER-1.pdf

Wu, Baichao; Tang, Aiping; Wu, Jie (2016, March): Modeling Cascading Failures in Interdependent Infrastructures Under Terrorist Attacks. *Reliability Engineering & System Safety,* 147, 1-8. DOI: https://doi.org/10.1016/j.ress.2015.10.019

Wukich, Clayton (2020, September): More Monitoring, Less Coordination: Twitter and Facebook Use Between Emergency Management Agencies. *Journal of Homeland Security and Emergency Management*, 17(3), Article 20200007. DOI: https://doi.org/10.1515/jhsem-2020-0007

Yavetz, Gal; Bronstein, Jenny (2023, September): Cities Under Fire: Crisis Communication on Home Front Versus Frontline Cities' Facebook Pages During Operation "Guardian of the Walls". *Journal of Contingencies and Crisis Management*, 31(3), 421-430. DOI: https://doi.org/10.1111/1468-5973.12448

Zager, Philip (2017, February): Bringing COIN to the Airport: On the Effectiveness of the "Muslim Ban". *Small Wars Journal*. URL: https://archive.smallwarsjournal.com/jrnl/art/bringing-coin-to-the-airport-on-the-effectiveness-of-the-%E2%80%9Cmuslim-ban%E2%80%9D

Zammit, Andrew (2017, October): New Developments in the Islamic State's External Operations: The 2017 Sydney Plane Plot. *CTC Sentinel*, 10(9), 13-18. URL: https://ctc.westpoint.edu/wp-content/uploads/2017/10/CTC-Sentinel_Vol10Iss9-21.pdf

Zammit, Andrew (2020, April): Operation Silves: Inside the 2017 Islamic State Sydney Plane Plot. *CTC Sentinel*, 13(4), 1-13. URL: https://ctc.westpoint.edu/wp-content/uploads/2020/04/CTC-SENTINEL-042020.pdf

Zhao, Xinyan; Zhan, Mengqi Monica; Liu, Brooke Fisher (2019, December): Understanding Motivated Publics During Disasters: Examining Message Functions, Frames, and Styles of Social Media Influentials and Followers. *Journal of Contingencies and Crisis Management*, 27(4), 387-399. DOI: https://doi.org/10.1111/1468-5973.12279

Żywucka-Kozłowska, Elżbieta; Broniecka, Rossana (2024): Security Threats to Port Critical Infrastructure. *Cybersecurity and Law,* 12(2), 273-281. DOI: https://doi.org/10.35467/cal/188576

## Grey Literature

Ackerman, Gary et al. (2007, January): *Assessing Terrorist Motivations for Attacking Critical Infrastructure*. (Lawrence Livermore National Laboratory Technical Report). DOI: https://doi.org/10.2172/902328

Allison, Benjamin V. (2022, December): *Deadly Detours: Why Terrorists Do Not Attack US Bridges and Tunnels.* (ICCT Research Paper). URL: https://www.icct.nl/publication/deadly-detours-why-terrorists-do-not-attack-us-bridges-and-tunnels

Andrae, Matthias et al. (2024, February): *Methodology for Numerical Simulations of Vehicle Impact on Security Barriers Considering Soil-Barrier Interaction*. (JRC Report). DOI: https://doi.org/10.2760/33565

Ashkenazi, Michael et al. (2013, February): *MANPADS – A Terrorist Threat to Civilian Aviation?* (BICC Brief No. 47). URL: https://www.bicc.de/Publications/Report/MANPADS---A-terrorist-threat-to-civilian-aviation/pu/12909

Atkins, Sean; Lawson, Chappell (2021, August): *Integration of Effort: Rethinking Cybersecurity for Critical Infrastructure.* (Belfer Center for Science and International Affairs, Policy Paper). URL: https://www.belfercenter.org/publication/integration-effort

Azani, Eitan; Atiyas Lvovsky, Lorena; Haberfeld, Danielle (2016, August): *Trends in Aviation Terrorism*. (ICT Articles). URL: https://www.ict.org.il/UserFiles/ICT-trends-aviation-terror-aug-16.pdf

Banks, William C.; Samuel, Katja (2019, September): *Hybrid Threats, Terrorism, and Resilience Planning*. (ICCT Perspectives). URL: https://www.icct.nl/publication/hybrid-threats-terrorism-and-resilience-planning

Barnosky, Jason Thomas et al. (2022, June): *Streamlining Emergency Management: Issues, Impacts, and Options for Improvement*. (RAND Research Reports, RR-A1440-5). DOI: https://doi.org/10.7249/RRA1440-5

Beckman, Luke (2023, June): *Navigating Poly-Crisis: The New Reality for Crisis Management in the United States*. (Belfer Center for Science and International Affairs Essay). URL: https://www.belfercenter.org/publication/navigating-poly-crisis-new-reality-crisis-management-united-states

Beckner, Christian (2015, January): *Risk-Based Security and the Aviation System: Operational Objectives and Policy Challenges.* (GW Center for Cyber & Homeland Security Issue Brief #2015-02). URL: https://www.jstor.org/stable/resrep20741

Bendiek, Annegret; Bund, Jakob; Kerttunen, Mika (2024, October): *The Attribution Dividend: Protecting Critical Infrastructure from Cyber Attacks*. (SWP Comment 2024/C 46). DOI: https://doi.org/10.18449/2024C46

Bergin, Anthony; Murphy, Clare (2015, April): *Sounding the Alarm: Terrorism Threat Communications with the Australian Public*. (ASPI Strategic Insights, No. 86). URL: https://www.aspi.org.au/report/sounding-alarm-terrorism-threat-communications-australian-public

Bipartisan Commission on Biodefense (2017, October): *Defense of Animal Agriculture*. (Report). URL: https://biodefensecommission.org/reports/defense-of-animal-agriculture

Bjelopera, Jerome P.; Elias, Bart; Siskin, Alison (2016, November): *The Terrorist Screening Database and Preventing Terrorist Travel*. (CRS Report for Congress R44678). URL: https://fas.org/sgp/crs/terror/R44678.pdf

Boeke, Sergei (2016, September): *First Responder or Last Resort? The Role of the Ministry of Defence in National Cyber Crisis Management in Four European Countries*. (ISGA Report). URL: https://scholarlypublications.universiteitleiden.nl/handle/1887/46615

Cheatham, Amelia; Roy, Diana; Labrador, Rocio Cara (2023, October): *U.S. Disaster Relief at Home and Abroad.* (CFR Backgrounder). URL: https://www.cfr.org/backgrounder/us-disaster-relief-home-and-abroad

Clarke, Yvette D. (Chair) (2021, October): *Transportation Cybersecurity: Protecting Planes, Trains, and Pipelines from Cyber Threats.* (Hearing presented before the House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation). URL: https://www.congress.gov/event/117th-congress/house-event/114172/text

Conway, Maura (2008): *Media, Fear and the Hyperreal: The Construction of Cyberterrorism as the Ultimate Threat to Critical Infrastructures*. (DCU Working Papers in International Studies, 5/2008). URL: http://doras.dcu.ie/2142/1/2008-5.pdf

Cook, Alistair D. B.; Ne, Foo Yen (2018, July): *Complex Humanitarian Emergencies and Disaster Management in Bangladesh: The 2017 Rohingya Exodus.* (NTS Report No. 11). URL: https://www.rsis.edu.sg/rsis-publication/nts/complex-humanitarian-emergencies-and-disaster-management-in-bangladesh-the-2017-rohingya-exodus

Cooper, Pete (2017, November): *Aviation Cybersecurity—Finding Lift, Minimizing Drag*. (Atlantic Council Report). URL: https://www.atlanticcouncil.org/in-depth-research-reports/report/aviation-cybersecurity-finding-lift-minimizing-drag

Cooper, Pete; Handler, Simon; Edwards, Safa Shahwan (2019, December): *Aviation Cybersecurity: Scoping the Challenge*. (Atlantic Council Report). URL: https://www.atlanticcouncil.org/in-depth-research-reports/report/aviation-cybersecurity-scoping-the-challenge-report

Demings, Val Butler (Chair) (2021, October-November): *20 Years After 9/11: Examining Emergency Communications*. (Hearing presented before the House Homeland Security Subcommittee on Emergency Preparedness, Response, and Recovery). URL: https://www.congress.gov/event/117th-congress/house-event/114112

Doty, Mary Bennett (2024): *The Accelerationism Events Dataset: Tactics, Techniques & Procedures*. (ARC Essay). URL: https://www.accresearch.org/accreports/the-accelerationism-events-dataset-tactics-techniques-amp-procedures

Doyle, Charles (2010, January): *Terrorist Attacks on Commercial Airlines: Federal Criminal Prohibitions.* (CRS Report for Congress, R41035). URL: https://sgp.fas.org/crs/terror/R41035.pdf

Edwards, Chris (2013, November): *Privatizing the Transportation Security Administration.* (Cato Institute Policy Analysis No. 742). URL: https://www.cato.org/policy-analysis/privatizing-transportation-security-administration

Farrell-Molloy, Joshua (2024, June): *"Natural" Connection: An Analysis of Eco-Fascism on Terrorgram*. (ARC Report). URL: https://www.accresearch.org/accreports/natural-connection-an-analysis-of-eco-fascism-on-terrorgram

Gaynor, Pete; Serino, Rich (Interviewees); Bruggeman, Nate (Interviewer) (2023, June): *Evolving the Emergency Management Enterprise to Meet a New Operational Reality: A Federal Perspective.* (Belfer Center for Science and International Affairs Conversations). URL: https://www.belfercenter.org/publication/evolving-emergency-management-enterprise-meet-new-operational-reality-federal

Gerstein, Daniel M.; Leidy, Erin N. (2024, April): *Emerging Technology and Risk Analysis: Artificial Intelligence and Critical Infrastructure.* (RAND Research Reports, RR-A2873-1). DOI: https://doi.org/10.7249/RRA2873-1

Ghenai, Chaouki (2024, May): *Countering the Growing Threat of Drone Attacks on Energy Infrastructure*. (New Lines Institute for Strategy and Policy, Policy Analysis). URL: https://newlinesinstitute.org/environmental-challenges/countering-the-growing-threat-of-drone-attacks-on-energy-infrastructure

Government Accountability Office (GAO) (2015, July): *Critical Infrastructure Protection: DHS Action Needed to Verify some Chemical Facility Information and Manage Compliance Process*. (Report to Congressional Requesters, GAO-15-614). URL: https://www.gao.gov/assets/gao-15-614.pdf

Grand-Clément, Sarah et al. (2021, October): *Executive Summary of the Study into Measures to Prevent Terrorist Attacks with Vehicles and Mitigate the Impacts Thereof.* (Report prepared by RAND Europe for the European Commission's Directorate-General for Migration and Home Affairs). URL: https://home-affairs.ec.europa.eu/whats-new/publications/study-measures-prevent-terrorist-attacks-vehicles-and-mitigate-impacts-thereof_en

Green, Mark E. (Chair) (2023, October): *The Role of Technology in Aviation Security.* (Hearing presented before the House Homeland Security Subcommittee on Transportation and Maritime Security). URL: https://homeland.house.gov/hearing/the-role-of-technology-in-aviation-security

Green, Mark E. (Chair) (2024, May): *Unmanned Aerial Systems and Emergency Response: The Impact of Drones and Other Emerging Technology on U.S. Law Enforcement.* (Hearing presented before the House Homeland Security Subcommittee on Emergency Management and Technology and the Subcommittee on Counterterrorism, Law Enforcement, and Intelligence). URL: https://homeland.house.gov/hearing/unmanned-aerial-systems-an-examination-of-the-use-of-drones-in-emergency-response

Hiraal Institute (2024, February): *The Price of Progress: Effects of the Clearing Operations on Businesses.* (Report). URL: https://hiraalinstitute.org/the-price-of-progress-effects-of-the-clearing-operations-on-businesses

Hollywood, John S. et al. (2024, March): *Keeping Soft Targets and Crowded Places Safe from Mass-Casualty Attacks: Insights from a Landscape Assessment.* (RAND Research Reports, RR-A2260-2). DOI: https://doi.org/10.7249/RRA2260-2

Jablanski, Danielle (2023, April): *Critical Infrastructure Cybersecurity Prioritization: A Cross-Sector Methodology for Ranking Operational Technology Cyber Scenarios and Critical Entities.* (Atlantic Council Issue Brief). URL: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/critical-infrastructure-cybersecurity-prioritization

Jenkins, Brian Michael (2012, August): *Aviation Security: After Four Decades, it's Time for a Fundamental Review*. (RAND Occasional Papers, OP-390-RC). URL: https://www.rand.org/pubs/occasional_papers/OP390.html

Johnson, Daryl; Beutel, Alejandro J. (2023, November): *Domestic Violent Extremist Targeting of the U.S. Electrical Transmission Grid.* (Newlines Institute for Strategy and Policy, Policy Report). URL: https://newlinesinstitute.org/nonstate-actors/domestic-violent-extremist-targeting-of-the-u-s-electrical-transmission-grid

Kane, Bridget R. et al. (2024, June): *Defending the Homeland Against Critical Infrastructure Attacks: Exploring a Hypothetical Campaign of Cascading Impacts.* (RAND Research Reports, RR-A2397-3). DOI: https://doi.org/10.7249/RRA2397-3

Kane, Bridget R. et al. (2024, June): *Threats to Critical Infrastructure: A Survey.* (RAND Research Reports, RR-A2397-2). DOI: https://doi.org/10.7249/RRA2397-2

Katko, John (Chairman) (2015, July): *Examining the Federal Air Marshal Service and its Readiness to Meet the Evolving Threat.* (Hearing presented before the House Homeland Security Subcommittee on Transportation Security). URL: https://www.congress.gov/event/114th-congress/house-event/103733/text

Katko, John (Chairman) (2015, September): *Safeguarding our Nation's Surface Transportation Systems Against Evolving Terrorist Threats.* (Hearing presented before the House Homeland Security Subcommittee on Transportation Security). URL: https://www.congress.gov/event/114th-congress/house-event/103918

Kayyem, Juliette (2022, February): *Emergency Management in North America.* (Working Paper; Belfer Center for Science and International Affairs / Wilson International Center for Scholars). URL: https://www.belfercenter.org/publication/emergency-management-north-america

Klein, Kevin; Talmadge, Shawn (Interviewees); Bruggeman, Nate (Interviewer) (2023, June): *Evolving the Emergency Management Enterprise to Meet a New Operational Reality: A State Perspective*. (Belfer Center for Science and International Affairs Conversations). URL: https://www.belfercenter.org/publication/evolving-emergency-management-enterprise-meet-new-operational-reality-state-perspective

Krill, Ilana; Clifford, Bennett (2022, September): *Mayhem, Murder, and Misdirection: Violent Extremist Attack Plots Against Critical Infrastructure in the United States, 2016-2022*. (GW Program on Extremism / NCITE Report). URL: https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/CriticalInfrastructureTargeting09072022.pdf

Leese, Matthias; Wildi, Lisa (2017, May): *Security Measures at Zurich Airport*. (CSS Analyses in Security Policy, No. 208). URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse208-EN.pdf

Lewis, James; Hewitt, James; Marsden, Sarah (2022, October): *The Psychological Effects of Criminal Justice Measures: A Review of Evidence Related to Terrorist Offending.* (CREST Report). URL: https://crestresearch.ac.uk/resources/the-psychological-effects-of-criminal-justice-measures

Lewis, James; Marsden, Sarah (2020, November): *Terrorism-Related Simulations.* (CREST Report). URL: https://crestresearch.ac.uk/resources/terrorism-related-simulations

Lin, Christina (2016, April): *New Airliner Threat: Arming Syrian Jihadists with US Anti-Aircraft Missiles.* (ISPSW Strategy Series: Focus on Defense and International Security, Issue No. 416). URL: https://www.ispsw.com/wp-content/uploads/2016/04/416_Lin.pdf

Lindsay, Bruce R. (2023, March): *Stafford Act Assistance and Acts of Terrorism.* (CRS Report for Congress, R44801). URL: https://sgp.fas.org/crs/homesec/R44801.pdf

Loadenthal, Michael (2024): *Introducing the Accelerationism Events Dataset.* (ARC Essay). URL: https://www.accresearch.org/accreports/introducing-the-accelerationism-events-dataset

Lopes, Marta (2020, December): *Responding to a Terror Attack: A Strong Cities Toolkit.* (ISD Report). URL: https://www.isdglobal.org/isd-publications/responding-to-a-terror-attack-a-strong-cities-toolkit

Malone, Iris; Strouboulis, Anastasia (2022, April): *Emerging Risks in the Marine Transportation System (MTS), 2001-2021.* (NCITE Report). URL: https://digitalcommons.unomaha.edu/ncitereportsresearch/27

McCaul, Michael T. (Chair) (2015, July): *Aviation Security Challenges: Is TSA Ready for the Threats of Today?* (Hearing presented before the House Committee on Homeland Security). URL: https://www.congress.gov/event/114th-congress/house-event/103805

McCaul, Michael T. (Chair) (2015, October): *Reform and Improvement: Assessing the Path Forward for the Transportation Security Administration.* (Hearing presented before the

House Committee on Homeland Security). URL: https://www.congress.gov/event/114th-congress/house-event/104038

McKay, Shawn; Hartnett, Gavin S.; Held, Bruce (2022, March): *Airline Security Through Artificial Intelligence: How the Transportation Security Administration Can Use Machine Learning to Improve the Electronic Baggage Screening Program.* (RAND Expert Insights, PE-A731-1). DOI: https://doi.org/10.7249/PEA731-1

Miller, Erin (2016, March): *Terrorism in Belgium and Western Europe; Attacks Against Transportation Targets; Coordinated Terrorist Attacks.* (START Background Report). URL: https://www.start.umd.edu/pubs/START_BelgiumTransportationCoordinatedAttacks_BackgroundReport_March2016.pdf

Miller, Erin (2016, June): *Terrorist Attacks Targeting Critical Infrastructure in the United States, 1970-2015.* (Report to the U.S. Department of Homeland Security). URL: https://www.start.umd.edu/publication/terrorist-attacks-targeting-critical-infrastructure-united-states-1970-2015

NATO Centre of Excellence Defence Against Terrorism (NATO COE-DAT) (2019): *Crisis Management in Terrorism*. (Seminar Report). URL: https://www.coedat.nato.int/publication/courseconfpapers/01-CIMIT_Seminar_Report.pdf

NATO Centre of Excellence Defence Against Terrorism (NATO COE-DAT) (2019, December): *Strengthening the Security and Resilience of NATO and Partner Nation Critical Infrastructure Against Terrorist Attacks: Lessons Learned Workshop.* (Report). URL: https://www.coedat.nato.int/publication/workshop_reports/09-CISR_LL_WS_Report_DD_v02_final.pdf

NATO Centre of Excellence Defence Against Terrorism (NATO COE-DAT) (2022): *SOF Roles in Crisis/CT Management Seminar*. (Seminar Report). URL: https://www.coedat.nato.int/publication/courseconfpapers/05-SOF_Roles_inCT_Crisis_ManagementReport.pdf

NATO Centre of Excellence Defence Against Terrorism (NATO COE-DAT) (2022, October): *Good Practices in Countering Terrorism in Maritime Domain.* (Seminar Report). URL: https://www.coedat.nato.int/publication/courseconfpapers/09-MARITIME_DOMAIN_SEMINAR(2023).pdf

Parfomak, Paul W. (2008, September): *Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options.* (CRS Report for Congress, RL33206). URL: https://sgp.fas.org/crs/homesec/RL33206.pdf

Payne, Leslie Adrienne et al. (2024, December): *Mentorship Efforts Within the Federal Emergency Management Agency's Incident Workforce.* (RAND Research Reports, RR-A2964-1). DOI: https://doi.org/10.7249/RRA2964-1

Power, Nicola et al. (2023, December): *Bridging the Principle-Implementation Gap: Evaluating Organisational Change to Achieve Interoperability Between the UK Emergency Services.* (CREST Short Report). URL: https://crestresearch.ac.uk/resources/the-psychology-of-interoperability-study-two

Power, Nicola et al. (2023, December): *The Psychology of Interoperability: A Systematic Review of Joint Working Between the UK Emergency Services.* (CREST Paper). URL: https://crestresearch.ac.uk/resources/the-psychology-of-interoperability-a-systematic-review

Propp, Kenneth (2021, July): *Avoiding the Next Transatlantic Security Crisis: The Looming Clash Over Passenger Name Record Data*. (Atlantic Council Issue Brief). URL: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-looming-clash-over-passenger-name-record-data

Romm, Madeline (2024, September): *Advancements in the Connection Between Internet of Things (IoT) and Geospatial Technologies.* (NCITE / START Rapid Review No. 2). URL: https://digitalcommons.unomaha.edu/ncitereportsresearch/89

Rutter, Megan (2024, September): *Advancements in Open-Source Geospatial Technologies and the Exploitation by Bad Actors.* (NCITE / START Rapid Review No. 3). URL: https://digitalcommons.unomaha.edu/ncitereportsresearch/88

Samuel, Thomas Koruth (2008): *Aviation Security in Malaysia*. (SEARCCT Study). URL: https://www.searcct.gov.my/wp-content/uploads/2020/03/Aviation-Security-In-Malaysia.pdf

Shay, Shaul (2021, January): *Al Shabaab and the 9\11 Style Terror Plot*. (ICT Articles). URL: https://www.ict.org.il/images/Al%20Shabaab%20and%20911.pdf

Sin, Steve; Washburn, Rhyner (2023, September): *Significant Multi-Domain Incidents Against Critical Infrastructure (SMICI) Dataset*. (START Research Brief). URL: https://www.start.umd.edu/publication/significant-multi-domain-incidents-against-critical-infrastructure-smici-dataset

Slakaityte, Veronika; Surwillo, Izabela (2024, October): *Protecting EU's Critical Infrastructure: The Fight Intensifies in the Cyber Realm*. (DIIS Policy Brief). URL: https://www.diis.dk/en/research/protecting-eus-critical-infrastructure-the-fight-intensifies-in-the-cyber-realm

Stewart, Grace; Doty, Mary Bennett (2024, May): *The Accelerationist Events Dataset: A Demographic Examination.* (ARC Essay). URL: https://www.accresearch.org/accreports/the-accelerationist-events-dataset-a-demographic-examination

Thompson, Bennie G. (Chair) (2019, April): *Supporting a Fact-Based Approach to Preventing Terrorist Travel to the United States*. (Hearing presented before the House Homeland Security Subcommittee on Intelligence and Counterterrorism). URL: https://www.congress.gov/event/116th-congress/house-event/109230

Thompson, Bennie G. (Chair) (2019, October): *One Year Later: Implementation of the TSA Modernization Act.* (Hearing presented before the House Homeland Security Subcommittee on Transportation and Maritime Security). URL: https://democrats-homeland.house.gov/activities/hearings/one-year-later-implementation-of-the-tsa-modernization-act

Thompson, Bennie G. (Chair) (2022, September): *Federal Building Security: Examining the Risk Assessment Process.* (Hearing presented before the House Homeland Security Subcommittee on Oversight, Management, and Accountability). URL: https://www.congress.gov/event/117th-congress/house-event/115143

Treverton, Gregory F. (Ed.) (2011): *Comparing Early Warning Across Domains.* (CATS Workshop Report). URL: https://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-2265

United Nations Counter-Terrorism Committee Executive Directorate (CTED) (2017, March): *Physical Protection of Critical Infrastructure Against Terrorist Attacks*. (CTED Trends Report). URL: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted-trends-report-march-2017-final.pdf

Wild, Hannah; Amoroso, Paul (2024, November): *Improving Point of Injury Trauma Care for IED Victims*. (Small Arms Survey Briefing Paper). URL: https://www.smallarmssurvey.org/resource/improving-point-injury-trauma-care-ied-victims

*Judith Tinnes has a background in Information Science. Dr Tinnes works for the Leibniz Institute for Psychology (ZPID) in an open-access publishing programme for scholarly journals. Additionally, she serves as Information Resources Editor to 'Perspectives on Terrorism'. In her editorial role, she regularly compiles bibliographies and other resources for Terrorism Research and runs the execution monitoring project 'Counting Lives Lost' (CLL).*

PERSPECTIVES ON TERRORISM

Book Review

# Review Essay: The Psychology of Terrorism

Reviewed by Joshua Sinai*

Volume XIX, Issue 1
March 2025

ISSN: 2334-3745

* *Corresponding author: Joshua Sinai, Perspectives on Terrorism, email: joshua.sinai@comcast.net*

**John Horgan, *Terrorist Minds: The Psychology of Violent Extremism from Al-Qaeda to the Far Right*** (New York, NY: Columbia University Press, 2024), 248 pp., US $ 120.00 [Hardcover], US $ 30.00 [Paperback], ISBN: 978-0-2311-9839-4.

**J. Reid Meloy and Jens Hoffmann (Eds.), [Second Edition], *International Handbook of Threat Assessment*** (New York, NY: Oxford University Press, 2021), 760 pp., US $ 165.00 [Paperback], ISBN: 978-0-1909-4016-4.

**Eric D. Shaw, *The Psychology of Insider Risk: Detection, Investigation and Case Management*** (Boca Raton, FL: CRC Press, 2023), 222 pp., US $ 140.00 [Hardcover], US $ 56.99 [Paperback], ISBN: 978-0324-8248-4.

Terrorism studies is a multidisciplinary endeavour, with scholars focusing on a wide range of topics such as radicalisation, how individuals are recruited into terrorist networks, their ideologies and agendas, how they are organised and led, their decision to employ certain types of weapons (as opposed to others), how they operate in physical environments and in cyberspace, and their selection of targets, among many other research questions. Within the scholarly literature on the psychology of terrorism, there are at least five challenges that have not been adequately addressed. First, there is a lack of consensus about defining terrorism, and specifically whether it involves only attacks against non-combatant civilians and/or armed combatants to achieve their political objectives. Granted, this is a challenge shared by scholars far beyond the realm of psychology, but here it is particularly significant, as a consistent definition is needed when examining the psychological characteristics of the motivations, agendas, behaviours, and targeting mindsets of those who engage in terrorist-type attacks against civilians and combatants. A second challenge is the lack of consensus about the psychology of those who become ideologically-driven terrorists. For instance, some authors consider them to be primarily rational actors intent on achieving political objectives, while others describe them as psychologically disordered individuals who grasp on to nihilistic extremist ideologies in order to justify their violent acts. A third challenge involves the widespread debates and disagreements among scholars about whether it is possible to psychologically profile those who become terrorists. A fourth challenge involves a tendency to overlook other related categories of violent attackers, such as psychologically disordered active shooters and 'insider threat' actors (i.e. they are known to some of their targeted adversaries), resulting in the discipline's ignoring a substantial literature of inter-related violent actor categories that should inform comparative analyses in studies on the psychology of terrorism. And a fifth challenge involves the need for practically useful diagnostic tools, tables, and checklists that can be applied to examine these issues in a structured analytic way.

To examine how these issues and problems are reflected in the contemporary research literature, three recently published books have been selected that focus on similar and different aspects of the psychology of terrorism.

In *Terrorist Minds*, John Horgan, insightfully explains that "Psychologists study behaviour – what people do and how they do it – and then we try to interpret *why* they do it" (p. xv). As a social process, he adds, "people *choose* to engage in terrorist activity...because they believe they are acting on behalf of a community that will embrace them for doing so. They feel they have a role to play in changing something much bigger than themselves, their immediate group, or the broader community from where they enjoy support" (p. xv). Regarding the second challenge described above, however, this characterisation sounds overly rational and altruistic, as there are many cases of individual members of terrorist groups (such as al-Qaeda, the Islamic State, Boko Haram, and Hamas), who have clearly embraced (and in some cases enthusiastically spread) nihilistic extremist ideologies, which makes Horgan's characterisation appear uncritical.

In explaining *who* becomes a terrorist and *why*, Horgan writes that there are multiple drivers that characterise those who might join a group or become lone actors, which leads him to reject the notion of a single psychological profile (pp. 45-50). He does cite a study that found that "[m]ore than half of the single-issue terrorists displayed some evidence of a history of mental illness" (p. 45). But while he acknowledges psychologist Randy Borum's three factors that characterise those who become violent extremists — antipathy towards a target group, creating a justification and mandate for violent action, and removing social and psychological barriers to inhibit violent action (p. 76) — Horgan nevertheless argues that "we have difficulty establishing how they relate to one another…" (p. 76). In the final chapter, Horgan concludes that despite all the studies on the psychology of terrorism "We know more about who participates in various activities that constitute terrorism than about what motivates them" (p. 163). Clearly, as Horgan acknowledges, this field of inquiry has made progress, but still has much room for improvement.

As a comprehensive overview of the psychology of terrorism, two excellent chapters discuss the processes of disengagement and reintegration of former terrorists into society, and how psychologists 'talk to terrorists', including those incarcerated, to gain insights into their motivations and actions. However, regarding the fourth challenge discussed earlier, Horgan focuses exclusively on individuals who become terrorists, but not on related violent assailant lone actors, such as the categories of psychologically disordered active shooters and violent insiders, such as those who engage in workplace violence, who are also driven by extremist ideologies (however outlandish and bizarre). And regarding the fifth challenge, the book does not provide any diagrams, tables, or checklists that could be used to profile those who might be on the trajectory toward becoming terrorists, as he argues that such individuals are too multi-varied to profile. In conclusion, despite the challenges discussed earlier, throughout the volume Horgan is masterful in explaining his thinking processes on these issues, which is helpful in educating students and analysts on how to analyse them, making this a valuable textbook on the psychology of terrorism.

Meanwhile, two other recent books address the aforementioned need for practically useful diagnostic tools. The first is an edited volume by J. Reid Meloy and Jens Hoffmann, *The International Handbook of Threat Assessment*, with an impressive collection of contributors who are practitioner members of the Association of Threat Assessment Professionals (ATAP).[1] As practitioner psychologists, they apply diagnostic tools to examine the profiles and trajectories of susceptible individuals, who are primarily lone actors, who might be situated along the trajectory into targeted violence, including terrorism. These tools include a widely applied framework developed by Frederick S. Calhoun and Stephen W. Weston, which they discuss in their chapter on "Rethinking the Path to Intended Violence," on the five pre-incident phases in targeted violence of grievance. These include: triggers; ideation (fantasising about taking revenge); research and planning (deciding how, where, and when to attack); preparation (such as acquiring a weapon); and breaching (transporting themselves to the target), which lead to the final sixth phase of their attack (pp. 392-404).

In terms of risk factors to engaging in targeted violence, the chapter by Monica Lloyd, "Making Sense of Terrorist Violence and Building Psychological Expertise," cites three widely used diagnostic tools in the field of terrorism risk assessment (pp. 624-629). The first—the Terrorist Radicalization Assessment Protocol (TRAP-18)—was developed by Meloy and is designed to code eight proximal warning behaviours and ten distal (or distant) characteristics.[2] The second—Extremist Risk Guidance (ERG22+)—was developed by the UK Department of Justice, and consists of 22 items across three dimensions: Engagement, Intent, and Capability. When correlated these dimensions are rated as being *strongly present/significant*, *partly present/*

*some*, or *not present/minimal*.[3] The third, Violent Extremism Risk Assessment 2 Revised (VERA-2R), was developed by The Netherlands Ministry of Justice and Security.[4] It consists of 34 risk-supporting and risk-mitigating indicators that are assessed to provide a professional risk judgment of an individual's potential for becoming a violent extremist.

Another category of terrorist-related targeted violence involves violent insiders. In *The Psychology of Insider Risk*, Eric D. Shaw, a prominent clinical psychologist and former US government intelligence officer, defines insider threat actors as individuals "who knowingly betray their organizations" whether through espionage, sabotage, workplace violence, leaks, and theft of intellectual property (p. xv). For the purpose of this essay, the focus is on ideologically-driven terrorist insiders who carry out workplace violence-type attacks. With numerous cases of ideologically extremist terrorists targeting their workplaces, such as former US Army Major Nidal Hassan's attack against his fellow soldiers at Fort Hood, Texas (5 November 2009) and husband-and-wife Syed Rizwan Farook and Tashfeen Malik's mass shooting attack at Farook's workplace holiday party in San Bernardino, CA, on 2 December 2015, the shooters were known to at least some of their intended targets, making them 'insiders'.

Based on the data from the cases Shaw has examined, he finds that individuals who become insider threats can be profiled. They were "not normal, well-adjusted individuals," they had "significant symptoms of personality disorders," they had a "history of previous violations" of policy and procedures, they felt "victimized" and "disgruntled," and importantly, "[c]oworkers and/or family members were aware of the risks" they presented (pp. 10-11), which could have led to pre-emptive interventions if these suspicions had been reported to appropriate authorities.

As a clinical psychologist, the author developed a diagnostic tool, termed the Critical Pathway to Insider Risk (CPIR) framework, to assess and map the trajectory of susceptible individuals toward becoming insider threats. It consists of the five progressive phases of personal predispositions, stressors, concerning behaviours, problematic organisational responses to their suspicious behaviours, and crime scripts (i.e. the attack) (p. 17). These phases are accompanied by risk indicators that are scored as highly diagnostic, moderately diagnostic, and minimally diagnostic (pp. 167-169). Each phase includes intervention points to mitigate the progression into carrying out an attack.

When assessing the risk of individuals to become terrorist insiders, Shaw also utilises the VERA-2 and TRAP-18 risk scales, which he overlays onto the CPIR framework (p. 162). Of course, identifying a universally applicable "profile of a terrorist" has been a holy grail for psychologists for many decades. And while there are valid concerns that must be acknowledged about the potential for misuse and abuse of these risk assessment tools, there is clearly merit in the efforts described in both the *International Handbook* and Shaw's *Insider Risk* book.

In conclusion, the three books under review present different kinds of contributions to the research literature on the psychology of terrorism. Two of the books present diagnostic tools to examine the profiles of potential terrorists, while Horgan's book provides a broader overview of the many complexities of this field. Incorporating diverse approaches, including comparisons with related subcategories of active shooters and violent insiders, can help us appreciate what the broader landscape of research on the psychology of terrorism has to offer.

*Joshua Sinai is Book Reviews Editor for Perspectives on Terrorism*

## Notes

[1] Association of Threat Assessment Professionals, online at https://www.atapworldwide.org/

[2] J. Reid Meloy, (2018). “The operational development and empirical testing of the terrorist radicalization assessment protocol (TRAP–18).” *Journal of Personality Assessment,* 100(5), 483–492.

[3] Extremist Risk Guidance (ERG22+), UK Department of Justice. Online at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1145219/extremism-risk-guidance-22+.pdf

[4] “Violent Extremism Risk Assessment 2 Revised” (VERA-2R), Netherlands Ministry of Justice and Security. Online at: https://www.vera-2r.nl/

# Announcements

## Call for Nominations for a New Editor-in-Chief for *Perspectives on Terrorism*

James Forest will be transitioning out of the Editor-in-Chief position for *Perspectives on Terrorism* during the summer or fall of 2025. A new Editor-in-Chief of the journal will be selected by the journal's Steering Committee, comprised of leaders at the three institutions that now co-publish the journal: The International Centre for Counter-Terrorism (ICCT), the Institute of Security and Global Affairs (ISGA) at Leiden University, and the Handa Centre for the Study of Terrorism and Political Violence (CSTPV) at the University of St Andrews.

Nominations for Editor-in-Chief for *Perspectives on Terrorism* (including self-nominations) are welcome and can be sent via email to pt.editor@icct.nl. Once a new Editor-in-Chief has been selected, Prof. Forest and Managing Editor Anna-Maria Andreeva will work them to ensure a smooth transition and successful publication of the September and December issues of the journal.

## Special Section Ideas for 2025

We are exploring the possibility of publishing a "Special Section on Artificial Intelligence and Terrorism" in one of our issues planned for 2025. Please contact pt.editor@icct.nl if you are interested in contributing a Research Article, Research Note, Bibliography or Book Review Essay on that topic. Also, we invite suggestions for other topics about which the journal might consider publishing a Special Section. Please send those to the address noted above.

## Call for Book Reviewers

The Editorial Team at *Perspectives on Terrorism* is eager to expand our Book Review section to begin including reviews of books published in languages other than English. Each year, many books on terrorism and counterterrorism-related topics are published in French, German, Spanish, Chinese, and other languages that go largely unnoticed by English-speaking scholars. If you would be interested in contributing to this initiative, please contact pt.editor@icct.nl.

PT
PERSPECTIVES ON TERRORISM

Perspectives on Terrorism is a publication of the
International Centre for Counter-Terrorism
T: +31 (0) 70 763 0050
E: pt.editor@icct.nl
W: pt.icct.nl