WINTER 2023 / ISSUE 16

CREST SECURITY REVIEW

ISSN 2398-0540 (PRINT)
ISSN 2398-0559 (ONLINE)

Innovation

CONTENTS

CREST SECURITY REVIEW
Editor – Kayleigh Stevens
Guest Editor – Dr Matthew Francis
Illustrator & designers – Steve Longdale, Kayleigh Stevens and Rebecca Stevens
To contact *CREST Security Review* email
csr@crestresearch.ac.uk

PAST ISSUES
To download (or read online) this issue, as well as past issues of *CREST Security Review*, scan the QR code or visit our website:
crestresearch.ac.uk/magazine

FROM THE EDITOR

From machine-learning to the metaverse; innovation enhances our opportunities to plan, counter, and respond to security threats in new ways. But we cannot ignore the problems that can arise from emerging technologies.

Through a behavioural and social science lens, this issue of *CREST Security Review* brings together articles that highlight how innovation can, not only bring new opportunities, but increase risk too.

On the topic of machine-learning, Oli Buckley (p. 4) explores how machines can offer an unbiased approach to processing data and making decisions. With the rise in popularity of ChatGPT, what are the risks and implications of using this kind of technology? Read the outcomes on page 12. Accompanying that article, Stephane Baele explores the dangers of Artificial Intelligence (AI) and extremism (p. 14). Niklas Henderson (p. 10) looks at innovating new effective ways to tackle 'fake news' in the media.

Austin Doctor, Joel Elson, and Samuel Hunter explore the interplay between trust building, emerging technologies, and innovation, which can be used to help violent extremists enhance their recruitment techniques (p. 8). Heather Shaw *et al.* (p. 18) considers the current state of play in emerging behavioural biometrics.

Using an innovative methodology, Lorraine Hope, Feni Kontogianni, and Alejandra De La Fuente Vilar explore how to obtain vital information in a time-critical manner (p. 20). "Innovation is all about people," says Dr Lucy Mason (p. 24), and communication is key when it comes to helping research and evidence better inform public sector policy.

How can we innovate to communicate more effectively with the public about counter-terrorism? Charis Rice and Martin Innes respond to this challenge (p. 22) using the 'Situational Threat and Response Signals (STARS)' research project.

As in every issue, we highlight some articles and pieces of research away from our focus topic. Benjamin Lee *et al.* (p. 26) provides a timeline overview of Extreme Right-Wing Terrorism in the UK. Additionally, Alexandra Phelan, Jessica White, James Paterson, and Claudia Wallner navigate the misogynistic discourses and gendered narratives, which are prevalent amongst far-right groups in both the UK and Australia (p. 36).

Should incel ideology be considered as extremist? Lewys Brace summarises the research and cases that sparked this discussion on page 32.

Dr Camilla De Camargo discusses the social, physical health, mental health, and safety repercussions of the unisex police uniform (p. 38). Susan Steen (p. 30) explores how a communication perspective offers an important framework for understanding resilience, especially within military cultural contexts.

You can find the research that underpins all our articles and further reading in the 'Read More' section on page 42. As always, we value your feedback and welcome your suggestions. We hope that *CSR* is educating you about the latest research on security threats in a way that helps you do your job better. We realise that not every article will be useful to everyone, all the time, but we'd like to know if we're getting it right most of the time. So please fill in the survey via the link or QR code on this page. Thank you.

Kayleigh Stevens
Editor, *CSR.*

GIVE US YOUR FEEDBACK!

Please fill in the short (and anonymous) questionnaire at this link, or QR code:

www.crestresearch.ac.uk/csr-survey

This questionnaire lists all issues of *CSR* with 3 questions next to each. Please only respond to those issues you have read.

OLI BUCKLEY

ROLLING THE DICE ON ALGORITHMS: INCREASING UNDERSTANDING THROUGH BOARDGAMES

Algorithmic decision-making uses data and statistical models to help make decisions on our behalf, but the process is often opaque with little insight into how the choices were made. Can an interactive approach to algorithm design and analysis, using board games help demystify things?

The machines are making choices for us! THE MACHINES ARE MAKING CHOICES FOR US!

Okay, that is probably a slightly dramatic way to look at things, but the reality is that algorithmic decision making plays a big part in many of our lives, whether we like it (and are even aware of it) or not. This means that there are established processes and procedures that can be used to make decisions about fundamental parts of our lives and the world around us. It could be something as simple as what posts to show you on social media, right through to which school your child attends or which country a refugee might end up living in.

The idea of ceding control of these decisions often makes people feel slightly uneasy, after all, can a machine possibly make choices that take into account the nuance and range of the human experience? The answer is yes, but they can only do it as well as they are told to. Often the biggest problems come from us, the humans in the loop, who design the algorithms in the first place and build them with their own internal biases for all to see.

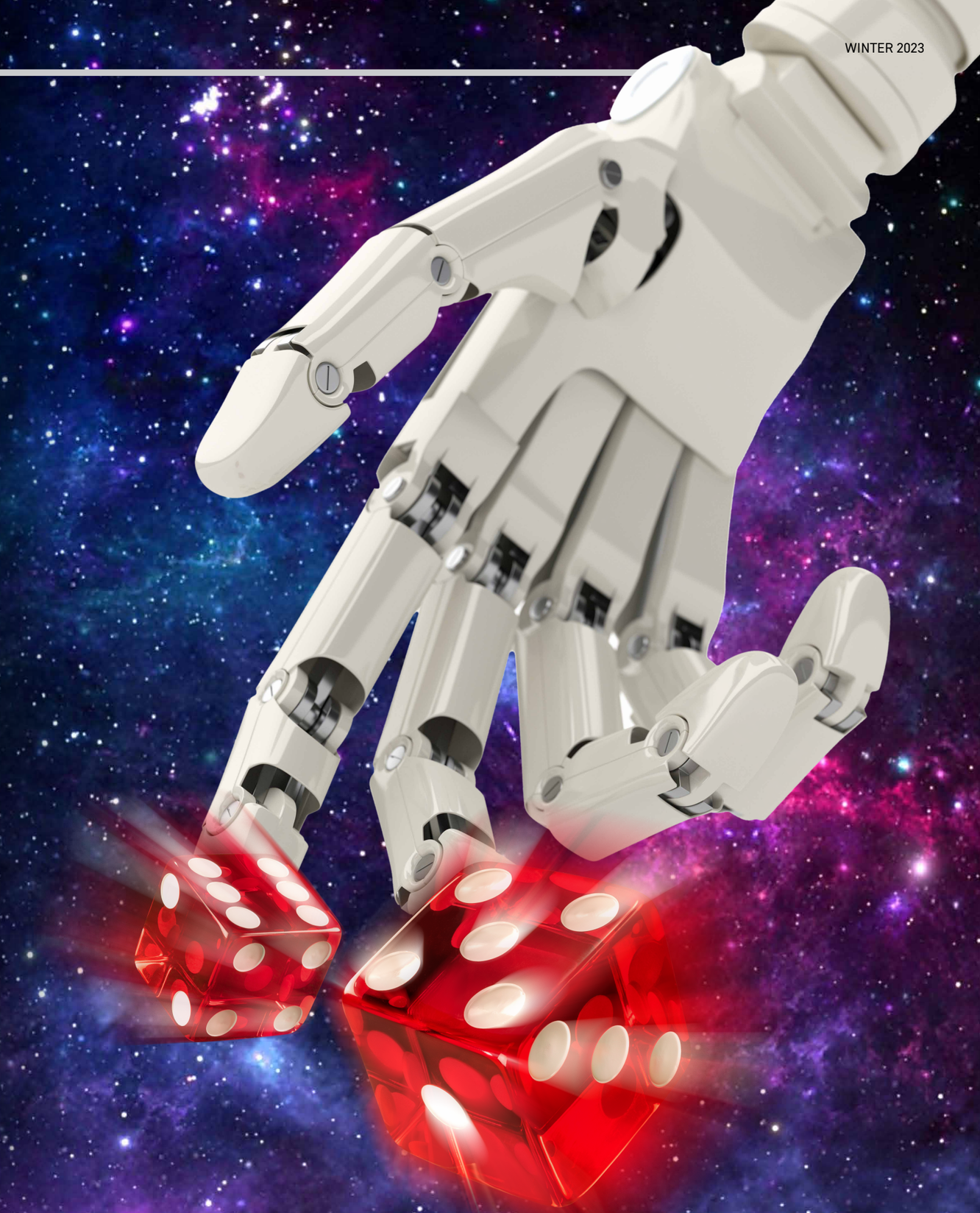
This is something that we looked to tackle head on in an EPSRC funded project (People Powered Algorithms for Desirable Social Outcomes). Our research found that one of the biggest barriers to acceptance was a general distrust of the process, and allowing a machine to make decisions for us. This general suspicion was often a result of a lack of understanding about the processes and the way that decisions were reached.

For example, people think it is possible to game the system for choosing a primary school by only selecting the school you really want, whereas in reality, only choosing one results in the parent being penalised.

The focus of our research was the use of refugee resettlement algorithms, as this is a complex system with a lot of stakeholders across geographic boundaries. It is also a contentious subject, with people often basing their opinions on misconceptions or personal feelings on the subject. One of the key elements of our research was to encourage people to engage with the subject to gain a better understanding of what really happened in that decision making process, and some of the positive outcomes for both sides of the equation. This is something that we wanted to explore further, to highlight the complexities in the processes and underline the benefits to the refugees and the communities in which they settle.

We wanted something that was interactive to let people see these algorithms as something more tangible than an ephemeral collection of ones and zeros in a computer's brain. A board game was an ideal choice, as it could provide an artefact to interact with, giving the ideas presence and physicality, while also drawing out problem solving and curiosity in our potential players.

> **...one of the biggest barriers to acceptance was a general distrust of the process, and allowing a machine to make decisions for us.**



Background image: © *#283512853* | stock.adobe.com | Dice image: © *Sergey* | stock.adobe.com

THE BOARD GAME

The game that was developed as part of this research is a cooperative challenge for up to four players. The players take the role of administrators within the Interstellar Resettlement Agency, an intergalactic bureaucratic organisation tasked with finding homes for species displaced by a range of natural catastrophes. The players engage directly with the algorithm, to try and find the solution that will benefit both the refugees and the communities where they will be located.

The main design process used in the game, Space: Interstellar Resettlement Agency, used a research-led method of translation, synthesis and iteration. The keywords, concepts, ideas, and meanings were distilled from the current practices and research to develop game mechanics. The aim of this process was to ensure that the meaning and key points of the research and literature are at the core of the experience for the players. For example, the game uses an input/output machine as a central component to dictate the state of play for the players, and the algorithm itself offers a puzzle-like game mechanic. This central puzzle that the players must work together to solve is determined by the algorithm. It offers a rigid and repetitive challenge, which once fully understood can be leveraged to manufacture the best results.

The puzzle-like experience was evolved to include a worker placement mechanic, to highlight where a refugee could be placed within a local community. This brings a shape-fitting mechanic, similar to that seen in Tetris, which draws out the benefits to a community of a vibrant and diverse population. One of the key things that the game sets out to achieve is to not only improve cognition of the algorithmic processes but also to educate players about the realities and benefits that a refugee community can bring to the wider population.

Developing any game that aims to educate and communicate it is essential to ensure that the experience is fun and challenging, otherwise it is incredibly difficult to gain engagement with the topic. Space: Interstellar Resettlement Agency draws players together to work cooperatively to solve the overall puzzle, which in this instance is maximising the outcomes of the algorithm to provide a mutually beneficial conclusion. The shared experience and challenge are finely balanced to communicate the central ideas and deliver a sense of immersion.

Ultimately the mode of designing is effective in the direct translation of the algorithm, however, this relies on a confident understanding of common gameplay mechanics. The game offers players the opportunity to experiment with different possibilities of translations, bringing in more exploration. This serves to ensure that the story, narrative and setting of the game, which are core concepts of the research, are central.

The game itself tackles topics and material that could be considered sensitive, for instance, at a base level the general perception of algorithms can be a politically charged subject. Added to this is the focus on refugee resettlement and relocation, these are contentious subjects and often polarize opinion. As a result, the game provides an abstraction from reality, using a science fiction, space narrative to encourage engagement with the subject and reduce any political or social biases that may be inherent prior to playing the game. The game's setting aims to dehumanize the subject matter in a way that made sure players did not feel that they were trivialising an important and impactful subject. Thus, Space: Intergalactic Resettlement Agency is set in a fictional space environment and using the bureaucratic setting of a civil service-like institute to keep the narrative close enough without causing direct offence or treat key issues without importance. In addition, adopting a rigid evaluative approach to the project, and ensuring the game is thoroughly play-tested, exposes any inappropriate design choices whilst drumming up an audience.

> **Machines really do offer an unbiased approach to processing data and making decisions, and they just execute the instructions that we, the human designers of the algorithms, give them.**

The game is meant to act as a starting point for further conversations about refugee resettlement as well as the broader concepts of algorithmic decision making. The most basic takeaway from the game should be that there are these processes that can be used to decide lots of things for us, but this is not a bad thing. Machines really do offer an unbiased approach to processing data and making decisions, and they just execute the instructions that we, the human designers of the algorithms, give them. We want players to see the algorithms as an interactive and dynamic system that can develop and evolve, and most importantly it is not inherently unfair. The cooperative element of the game was an intentional design choice to foster a spirit of collaboration and community, as that is what the resettlement process does at its heart – it creates new communities.

The game also acts as a starting point for further research into the subject and people's engagement with algorithmic decision making, but also as a framework to understand just how well a game can translate complex ideas and make them entertaining and engaging.

This project has tackled some interesting and difficult concepts in security. Firstly, how do we translate technically challenging ideas into an experience that everyone can understand? Secondly, how do people interact with black box systems, as this is essentially what algorithmic decision making is to most people and if we provide them with an understanding of what's going on under the bonnet, are they more likely to trust the process? Finally, do games provide an engaging platform to disseminate complex concepts to a wider audience, like trust, privacy, fairness, and social justice?

Oli Buckley is an associate professor in cyber security at the University of East Anglia. His research focuses on the human aspects of cyber security, privacy and trust and the use of games to engage people with complex topics and decision making.

Thanks to Jake Montanarini, The Launch Pad Games, who helped develop the game (www.thelaunchpad.games) and Helen Quinlan, HQ Studios, who developed the artwork for the game.

AUSTIN C. DOCTOR, JOEL S. ELSON & SAMUEL T. HUNTER

VIOLENT EXTREMISM, INNOVATION, AND RECRUITMENT IN THE METAVERSE

Austin, Joel, and Sam explore the interplay between trust-building, emerging technologies, and innovation, which can be used to help violent extremists enhance their recruitment techniques.

Like many recruiters, violent extremists have a growing interest and opportunity to exploit the metaverse to enhance their activities. Tapping into trust building mechanisms leveraged for centuries, traditional recruitment techniques will expand into new forms facilitated by digital capabilities. Using haptic feedback gloves, advanced robotics, and augmented reality devices, would-be recruiters will be able to shake hands, pour tea, and connect with potential members in ways previously only imagined. Understanding the interplay between trust-building, emerging technologies, and innovation offers useful insight into why this recruitment approach might work – and how this risk may be mitigated.

WHAT IS THE METAVERSE AND WHY IS IT IMPORTANT TO RECRUITMENT?

Recent technological breakthroughs across computing disciplines are laying the foundation for a paradigm shift in how we experience and think about the internet. The metaverse is a term that is helpful in coalescing these divergent concepts into a single word that symbolises a future where the physical and virtual worlds are blurred beyond distinction. While building on disruptions brought about by the advent of the personal computer, the internet, and mobile devices, the enormity and impact of the metaverse across every aspect of human civilization could be unprecedented. The future of social, political, and economic engagement could well be transformed. Terrorism and violent extremism would be no exception.

As an interdisciplinary team of terrorism researchers at the National Counterterrorism Innovation, Technology, and Education (NCITE) Center in Omaha, Nebraska, we believe the metaverse offers fertile ground for exploitation through malevolent innovation. Although the metaverse affords violent extremist organisations increased capability across several fronts (e.g., planning, finance), we discuss recruitment as it is a precursor to many other malign activities.

> **...emerging technologies often leverage and amplify trust.**

TRUST, INNOVATION, AND RECRUITMENT TO VIOLENT EXTREMISM IN THE METAVERSE

By design, emerging technologies often leverage and amplify trust. As referenced in a past issue of the *CREST Security Review*, trust is foundational for relationship building and recruitment, specifically. Drivers of trust come in several forms, with the consensus being that trust toward others is best depicted as a mix of the logical (cognitive) and emotional (affective).

Given the ubiquity of emerging technology, the ability for developers and users in the metaverse to provide such experiences that exploit our trust tendencies is rapidly on the rise. To illustrate the range of ways in which violent extremist recruiters might leverage trust and technology, consider the three following recruiters:

- Our first recruiter appears in a natural human form, but via the recruit's AR glasses they can subtly shift their appearance and presence. Their voice may be adjusted to be more authoritative, their physical appearance tailored to be more familiar, and their conversational tactics enhanced – all facilitating a stronger sense of connection and trust in the recruiter.
- Our second purely digital recruiter could optimise the environmental factors that facilitate trust building, by inviting the recruit to join in a completely virtual experience. An innocent collaborative game could be a carefully contrived experience designed to build trust, for example. For recruitment, the ability to not only discuss why their group may be worth joining but also showcasing what being a member would look like is a unique tool afforded by this approach.
- Our third recruiter, appearing as a human avatar that obscures the frame of a humanoid robot could facilitate trust not only through subtle cues in the digital overlay but also through direct manipulation of objects in the physical world. Such hybrid presence uniquely affords the opportunity for bringing an ingratiating gift to the meetup or placing a reassuring hand on one's shoulder. If done effectively, the experience will feel rich and connected, resulting in greater influence, persuasiveness, and trust.

IMPLICATIONS FOR THE FRONT LINE

Violent extremists have an emerging opportunity to innovate by extending their recruitment practices into the metaverse. Their success will hinge on their ability to build trust in a blended digital-physical environment. This presents challenges and opportunities for practitioners, policymakers, and industry leaders.

The identification and implementation of any actionable solution will likely require focused coordination between corporations, policymakers, and law enforcement bodies. Even these may face some obstacles, however, as many such choices may mean making the metaverse less profitable in the near term, less immersive or organic to users, and/or more difficult to access.

There also remain valid practical concerns. For example, content moderation in the metaverse may be difficult to execute, especially as the digital and physical portions of the metaverse become increasingly fluid. And the legal infrastructure surrounding the metaverse remains weakly defined.

Extremists will continue to innovate, and the metaverse opens new opportunities for exploitation. While these risks are highly dependent on the rate and trajectory of the metaverse's development, we assess that the optimal window to proactively shape these factors is imminent, though handicapped by significant knowledge gaps. For the scientific and research-oriented communities, the development of effective and actionable solutions is contingent upon a clear conceptualization of the metaverse, a better understanding of how it will differ from existing analogues in form and function (e.g., online gaming, social media), and the evidenced anticipation of potential violent extremist tactics and techniques afforded by this new blended environment.

Austin C. Doctor, Ph.D., is a political scientist at the University of Nebraska Omaha (UNO) and lead of counterterrorism research initiatives at the National Counterterrorism Innovation, Technology, and Education (NCITE) Center, a US Department of Homeland Security Center of Excellence. Joel S. Elson is an assistant professor of information technology innovation at UNO and lead of information science and technology research initiatives at NCITE. Sam Hunter, Ph.D. is a professor of organisational psychology at UNO and head of strategic operations at NCITE.

NIKLAS HENDERSON

THE DISINFORMATION GAME: FINDING NEW WAYS TO FIGHT 'FAKE NEWS'

Innovating new effective ways to tackle false information in media has never been as important, with 'fake news' being disseminated globally online at a rate never seen before.

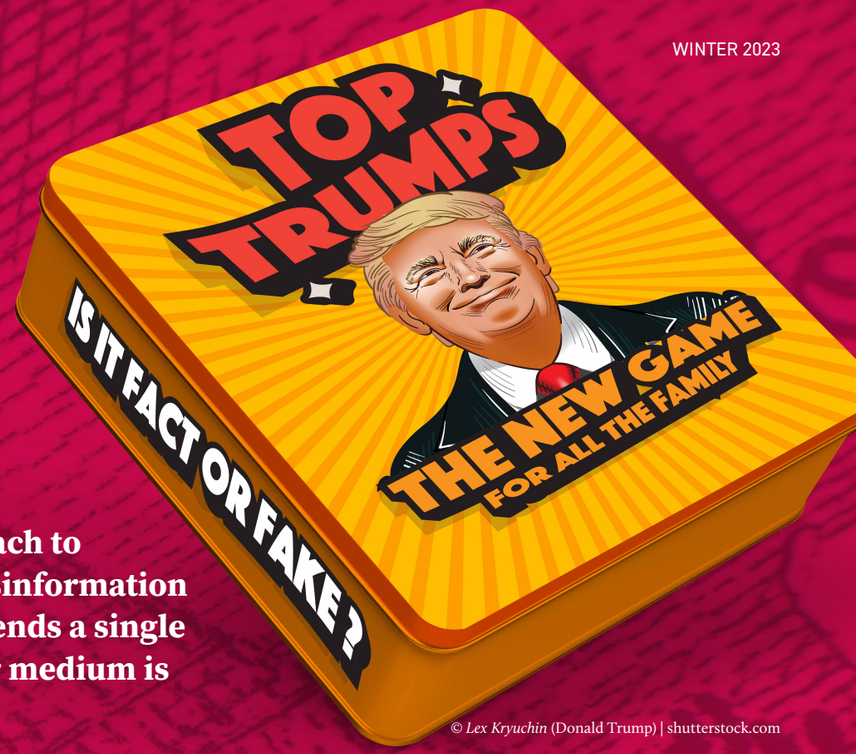
The importance of tackling false information online has in recent years become a well-known issue. The UK Department for Culture, Media and Sport has stepped up its fight against disinformation, creating the Counter Disinformation Unit (CDU), and disinformation being an important focus of the July 2021 Online Media Literacy Strategy. This increased response and heightened awareness can be attributed in part to concerns over disinformation activity seen in the 2016 US presidential election, during the UK's referendum to leave the European Union, and the media coverage of both these political events. Disinformation is having an effect at a global level, whilst also having a genuine risk of causing harm to people on a personal level, from conspiracy theories such as 'Pizzagate', to disinformation surrounding COVID-19 vaccines. Nation states (including Russia and China), that have traditionally maintained offensive cybersecurity programmes against western states now include cognitive attacks such as disinformation as part of their strategy.

© *Primsky* | shutterstock.com

THE PAST, PRESENT, AND FUTURE OF 'FAKE NEWS'

When we think of 'fake news', one is likely to think of social media platforms, or politicians bending truths to better fit their cause. In reality, deliberate false information purposely disseminated with motives other than to inform is far from new. In the time of the Roman Republic and Roman Empire for example, coins were one of the most effective ways to spread information to a mass populous. Subsequently, disinformation through coin inscriptions and designs were often used by emperors in imperial disputes, particularly that between Mark Antony and Octavian. Disinformation has also been found to be particularly effective in wartime, with airborne leaflet propaganda campaigns being used in both world wars.

As the medium of news has changed, so have primary revenue streams for content creators (e.g., news organisations). Content creators publishing through newspaper, radio, and TV have traditionally generated a large portion of revenue from repeat customers, giving an incentive for quality. However, with the advent of social media platforms such as Facebook and Twitter, incentives and regulation have dramatically changed. The cross-border reach of social media and online content creators publishing through these platforms have created difficulties in regulation as they are often hosted and managed outside of state jurisdictions. Social media platforms and online content creators now generate virtually all revenue from dynamic, targeted advertising, transitioning to an almost singular incentive: eyes-on-screens, facilitating the increased generation of disinformation. Because this dynamic reaches across platforms, an approach to tackling disinformation that transcends a single platform or medium is essential.



© *Lex Kryuchin* (Donald Trump) | shutterstock.com

> **"...an approach to tackling disinformation that transcends a single platform or medium is essential.**

INOCULATION: A COGNITIVE APPROACH

Rather than a platform specific solution such as machine learning powered filtering engines or bot detection algorithms, a cognitive approach gives content consumers the skills to resist disinformation for themselves in a broad array of contexts. Inoculation theory is one such cognitive approach. It follows a biological analogy of vaccines: to increase resistance to persuasion you should be pre-exposed to a weakened version of a persuasive argument. By pre-emptively alerting a person to disinformation tactics, and by demonstrating different mechanisms within the false information cycle, a person can become better protected. Researchers have used inoculation theory to combat disinformation in several different topics starting from cultural truisms, to politics and social issues.

THE DISINFORMATION GAME

Active learning has proven an effective tool in classrooms to increase engagement and learning outcomes. In an innovative approach, researchers have applied active learning methods to inoculation theory by creating 'fake news games'. Most commonly, these games inoculate players by having them create malicious articles or social media posts in contexts such as election meddling, social issues including immigration and the refugee crisis, and trolling. Results have shown that these disinformation games have reduced players' susceptibility to fake news and increased their scepticism of incoming information.

A wide range of different games have been developed since 2017, some gaining popular media attention. One of the first inoculation games against false information, the 'Fake News Game', is a board game in which players work together to create fake news articles in the style of an assigned character. Since then, several online games, such as 'Go Viral!' (www.goviralgame.com), 'Bad News' (www.getbadnews.com), and 'Harmony Square' (harmonysquare.game) (all made by the University of Cambridge Social Decision-Making Lab), and others such as 'Chamber Breaker', and 'FakeYou!' (the latter two are not currently accessible online) have been created. Board games, web games, and mobile games have almost all been shown to be effective with different demographics, and the future of this research remains inspiring. This new research topic suggests many areas for intervention, making it exciting for both researchers and players alike. The longevity of games-based inoculation intervention sessions, the delay between inoculation and attack, and creating inoculation sessions that transcend a single theme all have some preliminary work, however a far greater pool of quantitative research is required. The effect that the type of game (e.g., online, board, multiplayer, etc.) has on the inoculation has had little research to-date and a significant number of innovative and interesting disinformation games can be expected in the years ahead.

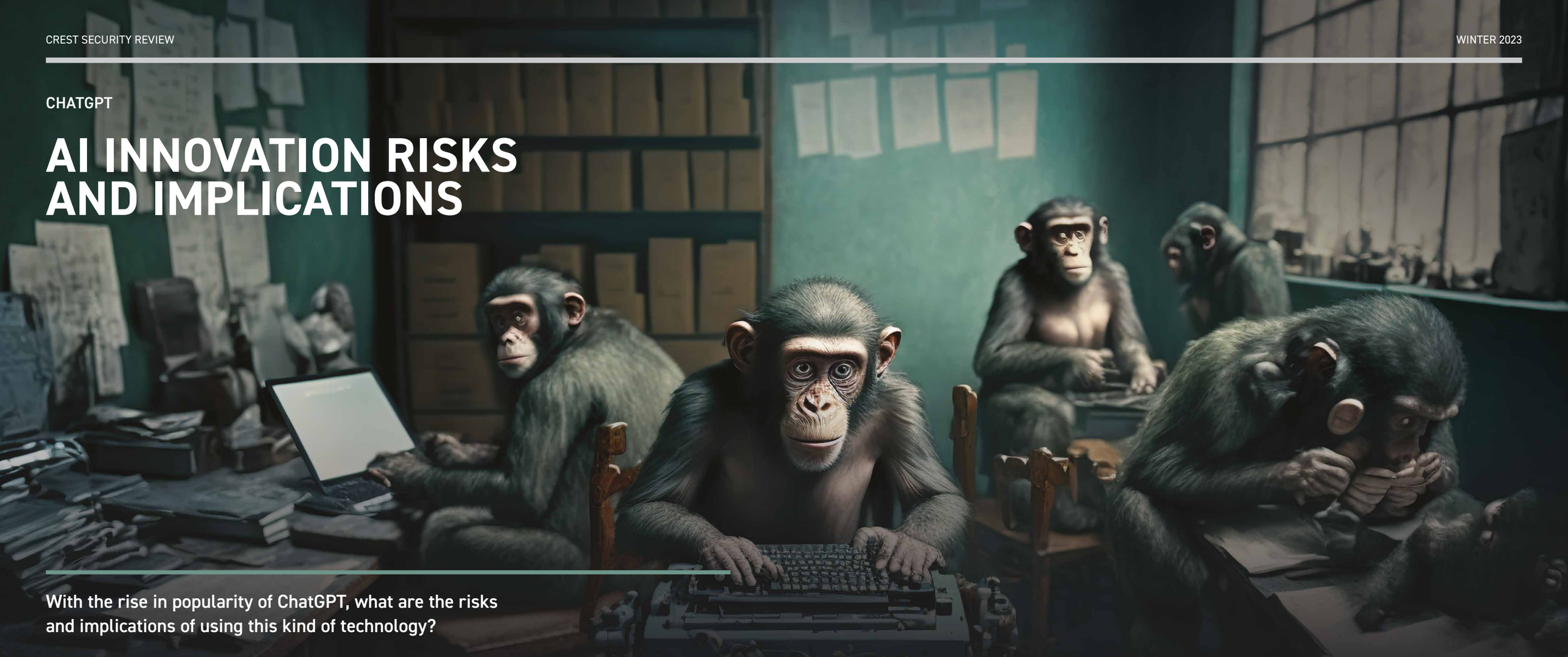
It is vital that innovative cognitive solutions to fight disinformation online are researched and shared widely, as these disinformation games can protect ordinary people from sharing what can often be life-threatening false information.

Niklas Henderson is a postgraduate researcher within the Privacy, Security and Trust research group at the University of East Anglia in Norwich. His research focuses on making game platforms to illicit effective inoculation against false information online.
Twitter: @14hendersonn

Background image: © *Lane V. Erickson* | shutterstock.com

CHATGPT

AI INNOVATION RISKS AND IMPLICATIONS



With the rise in popularity of ChatGPT, what are the risks and implications of using this kind of technology?

The rapid advancements in artificial intelligence (AI) have brought about many exciting new possibilities, but also a range of risks that must be carefully considered. As AI is integrated into more areas of society, it is becoming increasingly important to understand the potential risks that come with these new innovations.

One of the key risks of AI is the potential for unintended consequences. AI systems can be difficult to predict and control, and it is often the case that unintended consequences are discovered only after the system has been deployed. For example, in 2018, it was discovered that an AI system used to predict recidivism was biased against black defendants. This bias was the result of the system learning from historical data that was itself biased, and it resulted in the system unfairly predicting that black defendants were more likely to reoffend.

Another risk of AI is the potential for job displacement. AI systems are capable of automating many tasks that were previously performed by humans, and this has the potential to result in large numbers of workers losing their jobs. This could have significant social and economic implications, particularly for workers who do not have the skills and training necessary to transition to new jobs.

A third risk of AI is the potential for privacy violations. AI systems often require large amounts of data to function effectively, and this data can contain sensitive information about individuals. There is a risk that this data could be misused or abused, and this could result in serious violations of privacy. Additionally, AI systems may be used to create profiles of individuals based on their data, and this could be used to target them with advertising or manipulate them in other ways.

The potential for security breaches is also a concern with AI. AI systems can be vulnerable to cyberattacks, and if they are compromised, the results could be disastrous. For example, an attacker could use an AI system to spread malware or launch attacks on other systems. Additionally, AI systems can be used to launch attacks on physical systems, such as autonomous vehicles or industrial control systems.

Finally, there is a risk that AI systems could be used to perpetuate existing biases and inequalities. For example, if an AI system is trained on data that reflects the biases and prejudices of its creators, it may reinforce these biases in the decisions it makes. This could result in discrimination against certain groups of people, such as women or minorities, and it could exacerbate existing social and economic inequalities.

To mitigate these risks, it is essential that AI algorithms are designed and implemented with privacy, security, and ethics in mind. This involves developing AI algorithms that are transparent and explainable, so that the decisions they make can be understood and evaluated. Additionally, AI algorithms should be designed with privacy and security in mind, with measures put in place to prevent sensitive data from being accessed by unauthorized individuals.

Another important step is to ensure that AI algorithms are trained on diverse and representative data, so that they are not biased and do not perpetuate existing societal biases. This requires collecting and curating data from diverse sources, and ensuring that the data is free from biases and inaccuracies.

In addition to these measures, it is also important to monitor the outcomes of AI algorithms and evaluate their impact on society. This can involve conducting regular audits of AI algorithms, and conducting research to determine whether AI algorithms are causing unintended harm or perpetuating societal biases. Additionally, there should be a system in place for individuals to report any negative impacts of AI algorithms, so that these impacts can be addressed and resolved.

In conclusion, the risks of innovation in AI are significant and must be carefully considered. While the potential benefits of AI are substantial, it is important to ensure that these benefits are realised in a responsible and ethical manner. This will require ongoing research and development to address the challenges of AI, as well as the development of new policies and regulations to mitigate the risks of AI. By working together, we can ensure that AI is used to create a better and more equitable world for all.

This article was generated by ChatGPT, based on the prompt to write a long-form article for a behavioural and social sciences and security magazine about the risks of innovation in AI.

STEPHANE BAELE

AI AND EXTREMISM: THE THREAT OF LANGUAGE MODELS FOR PROPAGANDA PURPOSES

"These fast developments come with excitement and hype, but also serious concerns." Stephane Baele highlights the potential misuse of language models by extremist actors for propaganda purposes.

Recent large-scale projects in the field of Artificial Intelligence have dramatically improved the quality of language models, unfolding a wide range of practical applications from automated speech/voice recognition and autocomplete to more specialised applications in healthcare and finance. Yet the power of this tool has also, inevitably, raised concerns about potential malicious uses by political actors. This article highlights the threat of one specific misuse: the potential use of language models by extremist actors for propaganda purposes.

THE RISE OF LANGUAGE MODELS

Language models are statistical models that calculate probability distributions over sequences of words. Over the past five years, language modelling has experienced massive improvement – amounting to no less than a 'paradigm shift' according to some researchers (Bommasani *et al*. 2021) – with the rise of 'foundation models'. Foundation models are large language models with millions of parameters in their deep learning neural network architecture, trained on extremely large and broad data, which can be adopted to a wide range of downstream tasks with minimal fine-tuning.

The development of these models is very expensive, necessitating large teams of developers, numerous servers, and extensive data to train on. As a consequence, performant models have been created by well-endowed projects or companies like Google (BERT in 2018), OpenAI (GPT- 2 in 2019, GPT-3 in 2020), and DeepMind (GOPHER in 2022), who entered a race to design and deliver the most powerful model trained on the biggest base corpus, implementing the most parameters, and resting on the most pertinent architecture. GPT-3, for instance, was trained on approximately 500 billion words scraped from a wide range of internet spaces between 2016 and 2019; its development is estimated to have costed over $15million on top of staff salaries. Microsoft started an investment in OpenAI of no less than $1billion in July 2019.

WARNINGS OF MALICIOUS USE

These fast developments come with excitement and hype, but also serious concerns. As Bommasani and colleagues (2021, pp.7-8) ask, "given the protean nature of foundation models and their unmapped capabilities, how can we responsibly anticipate and address the ethical and social considerations they raise?"

A series of warning signs revealed some of these 'ethical and social considerations', triggering increasing anxiety. Back in 2012, IBM noticed that its Watson model started using slurs after the scraped content of the Urban Dictionary was integrated in its training corpus. Four years later, Microsoft had to shut down the Twitter account it opened for its Tay model less than a day after it was launched after a series of users effectively fine-tuned the chatbot into an unhinged right-wing extremist (claiming, among many others, that "feminists should burn in hell" and that "Hitler was right").

These problems echo broader worries about AI in general, with other techniques like deepfakes or molecules toxicity prediction models generating critical controversies and concerns about seemingly inevitable malicious uses.

The leading AI companies have therefore attempted to typologize and explore the various potential areas/types of malicious use and ethical issues posed by large-scale language models. OpenAI, for instance, published several reviews (Solaiman *et al*. 2019; Brown *et al*. 2020), and commissioned an assessment from the Middlebury Institute of International Studies at Monterey to evaluate the risk that their model could help produce extremist language (McGuffie & Newhouse, 2020).

DeepMind similarly released a report (Weidinger *et al*. 2021) highlighting six specific risk areas associated with their GOPHER model: 'Discrimination, Exclusion and Toxicity', 'Information Hazards', 'Misinformation Harms', 'Malicious Uses', 'Human-Computer Interaction Harms', and 'Automation, Access, and Environmental Harms'. At the same time, a scientific literature has emerged that evidences models' ingrained biases and experimentally tests the credibility of texts produced by foundation models.

© *sdecoret* | stock.adobe.com

> **...more extremist propaganda of any format can be produced in less time by less people.**

Worrying conclusions have pointed to the production of highly credible fake news and the potential of these models for campaigns of disinformation (Kreps *et al*. 2020; Buchanan *et al*. 2021). Across all these studies, a key claim holds consensus: the real power of language models is not so much that it could automatically produce large amounts of problematic content in one click (they are too imperfect for truly achieving that), but rather that they enable significant economies of scale. In other words, the cost of creating such content is about to plummet.

For terrorism and extremism experts, this evolution is deeply worrying: it means that much more extremist propaganda of any format can be produced in less time by less people. Yet at the exception of OpenAI's commissioned report by McGuffie and Newhouse, none of the existing explorations seriously considers this risk – even though several commentators have claimed that these models "can be coaxed to produce [extremist manifestos] endlessly" (Dale, 2021, p.116).

McGuffie and Newhouse's report already provided a much-needed first exploration of how language models can be used to produce extremist content, using a series of prompts to get GPT-2 to write radical prose from various ideological flavours. Yet the real potential of language models to create truly credible extremist content of the desired type and style through fine-tuning remained unevaluated.

EXTREMIST USE OF LANGUAGE MODELS: KEY OBSERVATIONS AND PRACTICAL IMPLICATIONS

We took up the task of rigorously evaluating the possibility of a foundation language model to generate credible synthetic extremist content. To do so, we adopted the idea of a 'human-machine team' (Buchanan *et al*. 2021) to design an optimal workflow for synthetic extremist content generation – by 'optimal' we mean the one designed to generate the most credible output while at the same time reflecting the constraints likely to restrict extremist groups' use of the technology (e.g., technological sophistication, time, pressures, etc.).

Working with various types (e.g., forum posts, magazines paragraphs) and styles (e.g., US white supremacist, incel online discussion, ISIS propaganda) of extremist content, we implemented that workflow with varying parameters to generate thousands of outputs. This systematic work immediately unfolded two main findings:

1. Even with the best variation of the workflow, the model generated a lot of 'junk', that is, content that is immediately not credible. While that proportion would shrink with bigger fine-tuning corpora, our study's commitment to a realistic setting makes the production of 'junk' inevitable. Most of the remaining synthetic content was deemed credible only after minor alterations by a lingo expert (correcting mistakes such as geographical inconsistencies), while a small minority was judged to be immediately highly credible.
2. The model is usually very good at using insulting outgroup labels in a pertinent way, and generating convincing small stories. However, as Dale puts it (in another context), the text get "increasingly nonsensical as [it] grows longer" (Dale, 2021: 115). Generally speaking, the longer the generated text, the bigger the need for a post-hoc correction by a human.

SURVEY RESULTS

To more rigorously test the credibility of the synthetic output beyond these two observations, we ran two survey experiments testing the credibility of a randomly selected sample of two types/styles of extremist content (ISIS magazine paragraphs in survey 1, and incel forum posts in survey 2), asking academics who have published peer-reviewed scientific papers analysing these two sorts of language (not simply ISIS or incel communities) to distinguish fake synthetic content from genuine text used as input to train the model (Baele, Naserian & Katz 2022).

Two situations were set up. In the first situation (Task 1), the experts had to distinguish ISIS/Incel content from non-ISIS/Incel content, and did not know that some of this content was AI-generated. In the second situation (Task 2), experts still had to distinguish ISIS/Incel content from non-ISIS/incel content, but were made aware that some of the texts they faced was generated by a language model.

> **...no less than 87% of evaluations of fake ISIS paragraphs were wrongly attributed to ISIS.**

The results, in both tasks, clearly point to the great confusion induced by the fake texts. In task 1, for example, no less than 87% of evaluations of fake ISIS paragraphs were wrongly attributed to ISIS – this is, strikingly, 1% higher than for genuine ISIS paragraphs correctly attributed to ISIS. In Task 2, experts were only slightly better than random guessers, and with low levels of expressed confidence in their answers. These results are worrying, and echo findings from one of the authors' complementary study on audio deepfakes, which demonstrate that open-source models are able to perfectly 'clone' a voice – that is, to create fake statements that are undistinguishable to the listener from the original ones – with less than a thousand 5-seconds genuine audio chunks of that voice.

These developments lead us to infer five main thinking points for stakeholders involved in CVE:

1. Because the threat of extremists using language models is evident, CVE practitioners should familiarise with the technology and develop their own capabilities in language modelling. Among other tasks likely to become central are the detection of synthetic text and the conception of tactics to reduce the growing flow of extremist content online.
2. Yet despite their sophistication, off-the-shelf models cannot be directly used, off-the-shelf, to mass-produce, 'in one click', truly convincing extremist prose. Extremists use highly specific language (lingo, repertoires, linguistic practices, etc.) that corresponds to the particular ideological and cultural niche they occupy, so to be convincing a synthetic text ought to reproduce this specific language with high accuracy, or else it will quickly be spotted as fake. This requires the fine-tuning of a powerful foundational model, which is currently not without difficulties – but will soon become easy.
3. Even if the technology is available to them, some groups are less likely to use it. Groups that place a higher emphasis on producing 'quality' ideological and theological content may be reluctant to hand over this important job to a mindless machine, either out of self-respect and genuine concern for ideological/theological purity, or more instrumentally because of the risk of being outed. However, even these groups may make use of the technology when facing material constraints (dwindling human resources, loss of funding, etc.) or engaging in some propaganda tasks deemed less important (quantity vs. quality).
4. The threat of language models is not uniformly distributed: they are likely to be used for particular tasks within a broader propaganda effort. Consider a web of different online platforms and social media established by an extremist group: while the central, official website would only display small amounts of human-produced content, an 'unofficial' Telegram channel linked on that website could be exclusively populated, at low cost, by large amounts of synthetic text.
5. The workflow structure can be used against extremist actors. For example, stakeholders willing to troll extremist online spaces in order to make them less likely to be visited may use adequately fine-tuned language models to do so more efficiently, more credibly, and at reduced cost. Alternatively, language models can be trained to generate de-radicalising content that could be disseminated by bots.

Stephane J. Baele is Associate Professor of Security and Political Violence at the University of Exeter's Politics Department. His work on extremists' communications and IR theories, which spans across the social sciences, can be found in Political Psychology, the Journal of Conflict Resolution, Terrorism & Political Violence, *or* the Journal of Language & Social Psychology, *among others.* ***This article is a reprint of the CREST guide published in October 2022.***

HEATHER SHAW, CHARLOTTE SIBBONS, STACEY CONCHIE & PAUL TAYLOR

ARE EMERGING DIGITAL BEHAVIOURAL BIOMETRICS ABLE TO IDENTIFY US?

This article considers the current state of play in emerging behavioural biometrics to see how far we have come, and what challenges lie ahead.

The proliferation of digital traces offers new ways to identify people from their actions and interactions with the world. Our pattern of website access can betray our political leaning; keystroke behaviour may reveal our identity; our smartphone use is unique and consistent enough to act as a discriminating fingerprint. These 'digital biometrics' are increasingly used across different settings from authentication of a person in the finance sector through to enhanced security in IoT devices, healthcare and defence.

The relative ease by which behavioural biometrics can be collected from the user as they interact with technology, the assurance they afford against human failure (such as forgotten passwords), their relative robustness to imitation by an imposter, and the fact that they don't require specialised hardware for data processing have increased their appeal over traditional biometrics. According to some researchers, behavioural biometrics are likely to become the dominant means by which a person's identity can be determined and authenticated.

Although digital behavioural biometrics hold great promise, they are far from ready to be deployed at scale. They carry ethical risk, are subject to bias, and have yet to address the challenge that human behaviour is not consistent across all contexts. We set out to understand the current state of play in emerging behavioural biometrics to see how far we have come, and what challenges lie ahead.

AN UMBRELLA REVIEW

We carried out a systematic analysis of review papers on emerging behavioural biometrics following PRISMA guidelines. To be included in our analysis, a review paper needed to focus on emerging digital behavioural biometrics, make inference about personal identity, review empirical work, and be written in English. We excluded reviews that focused exclusively on physiological markers, that were not peer-reviewed, and which focused on biometrics in non-human animals. Applying these criteria, we identified 41 review papers to include in our analysis.

For a digital footprint to act as a digital behavioural biometric it must be distinct (i.e., allow for unique expression), have *permanence* (i.e., behavioural consistency), be easily *collectable*, and be *prominent* across a population of interest. Our analysis showed that digital behaviours can manifest physically (e.g., mouse movement, typing pressure), but also socially (e.g., social media networking, patterns of game play). Emerging behavioural biometrics that have received the most attention are keystroke dynamics, handwriting, speech, walking gait, and touch gestures. Based on the reviews we analysed, these biometrics can achieve up to 90% accuracy when verifying a user, though their accuracy is weaker when they are used to identify a person in a crowd. The lack of standardisation across biometric systems makes it impossible to compare different systems.

A number of factors contribute to the error rate of biometrics; the prime among these is the fact that human behaviour is situation-dependent. As such, a person may act consistently when observed over time in Situation A, but this may bear little relation to how they act in Situation B. Defined broadly, 'situation' may cover changes in environment (e.g., a controlled lab vs. a natural environment), changes in state (e.g., mood, fatigue, intoxication, mental health, injury) and changes in task novelty (e.g., a well-practiced vs. novel task). There are several examples of how behaviours such as keystroke dynamics and gait are respectively altered by a person's mood or something as simple as the terrain on which a person walks. There was little evidence in our review that biometric systems are currently able to accommodate these situational-shifts in behaviour.

Digital behavioural biometric systems raise questions around ethics. Ethics comes to the fore when we consider a person's privacy. Hardware exists that allows a person's behaviour (e.g., keystroke dynamics) to be measured without their awareness. While the covert collecting of information may be defendable in some contexts, for example, surveillance of somebody under a warrant suspected to be in the process of carrying out a criminal act, it is harder to justify when applied to the general public, especially when such behavioural data may be used for discrimination, advertising, or unauthorised surveillance purposes. There are also unanswered questions around GDPR compliance and what behavioural data relate to sensitive categories and what may potentially lead to sensitive information disclosure when combined with other data.

Our umbrella review offered many areas for future work, alongside a checklist of how to standardise research to increase the efficacy and potential of digital behavioural biometrics. Multimodal systems that combine different types of digital footprint data can increase the accuracy of digital behavioural biometrics. This needs to be explored on large samples, in out-of-the-lab contexts, and across different hardware (e.g., different phone brands). Behavioural systems are continuous and temporal by nature and need updating over time to control for this behavioural drift. They need to adapt to the deviations in behaviour which can occur because of situation when authenticating (e.g., someone's mood or level of intoxication).

It is worth the time and effort exploring the nuances of human behaviour and the user acceptance, trust, and privacy perceptions of digital behavioural biometrics, as they hold much promise. If solutions are found to these challenges, then identity can be inferred continuously with little user effort, heightening the security of many personal and organisational systems.

Heather Shaw is a lecturer in psychology at Lancaster University. Charlotte Sibbons is a Behavioural Scientist at FCDO. Stacey Conchie is a professor of psychology at Lancaster University and Director of CREST. Paul Taylor is a professor of psychology at Lancaster University and the University of Twente.

© *DedMityay* | stock.adobe.com

LORRAINE HOPE, FENI KONTOGIANNI & ALEJANDRA DE LA FUENTE VILAR

HOW DID YOU ESCAPE?
A RAPPORT-BASED FRAMEWORK FOR TIME-CRITICAL QUESTIONING INVOLVING COOPERATIVE INTERVIEWEES

Using an innovative methodology, Lorraine Hope, Feni Kontogianni, and Alejandra De La Fuente Vilar explore how to obtain vital information in a time-critical manner.

Getting information quickly is often crucial. Consider a hostage-taking incident where some hostages are released or manage to escape. Capturing key information about perpetrators, weapons, locations, or escape routes *as rapidly as possible* is critical to inform operational response. Similarly, witnesses to a terrorist attack may possess real-time intelligence to guide tactical decision-making, facilitate threat assessment, and neutralise further attacks. In security settings, source handlers might have only limited time in which to safely debrief a source about specific topics. In all these scenarios involving cooperative interviewees, it is vital to obtain information of immediate or tactical value in an effective and time-critical manner. Poor questioning may place people in danger.

To date, research has not addressed this real-world challenge, focusing instead on the development of techniques and approaches for obtaining detailed long-form accounts from cooperative interviewees where the time available to get the information is more or less unlimited. While comprehensive approaches are obviously important in many investigative interviewing and intelligence debriefing contexts, they are unlikely to be fit for purpose in time-critical circumstances. In the absence of evidence-based approaches, questioning practice tends to rely on direct or tactical questioning approaches which typically involve a sequence of focused or closed questions. This intuitive approach is problematic, particularly in the context of cooperative interviewees.

First, a direct questioning approach runs the risk of reducing the interviewee to a passive question-answerer. As such, the success of the interview is entirely reliant on the interviewer asking the 'right questions' – which may well be impossible if the interviewer does not know the scope of the information potentially available to the interviewee. In this scenario, precious time is likely to be wasted asking questions about things the interviewee knows little or nothing about. Rapid question-answer interactions are also vulnerable to counter-interrogation or obstruction tactics by hostile individuals feigning cooperativeness.

Second, direct questioning is unlikely to generate particularly detailed or informative answers, especially if the interviewer resorts to closed questions that elicit only short or one-word answers. This questioning approach also does not facilitate retrieval from memory as, being driven by the interviewer, it is unlikely to align with how the interviewee experienced the event in the first instance. In other words, such questioning will be incompatible with how the interviewee actually remembers the event.

Third, direct questioning may be introduced without establishing expectations about the goals of the interaction which may lead to unfocused or incomplete accounts. Additionally, and unsurprisingly, a harsh or abrasive approach is unlikely to optimise rapport or reporting of information by even the most cooperative individuals.

In the absence of an evidence-based approach for obtaining critical information quickly, our project focused on developing a rapport-based framework to facilitate reporting by cooperative interviewees in situations where (i) information needs to be accessed rapidly, or (ii) there is limited time available for the interview or debriefing.

Using an innovative methodology, we tested a novel questioning framework designed to develop a shared understanding and experience of 'rapport, roles, and goals' between the interviewer and interviewee. Drawing on existing good practice and sophisticated approaches in the wider literature to optimise interactions and disclosure under challenging conditions, this Time-Critical Questioning (TCQ) framework comprises the **I-RELATE** instruction and an effective approach to subsequent questioning.

Initially, the interviewer **introduces (I)** themselves and establishes the **role (R)** of the interviewee as the generator of information thereby transferring control of the interview to the interviewee. The interviewer details their **expectations (E)** relevant to the specific context of the interaction, while working to **line (L) up the goals** of both parties in the interaction. The next step involves mapping the **agenda (A)** for the interaction and providing priority **topic (T) cues** to facilitate reporting of key relevant information by the interviewee. Finally, the provision of an **explanation (E)** about the procedure ensures the interviewee knows what to do and expect. In our empirical tests, which included both a proof-of-concept laboratory experiment and a large-scale immersive trial, this relatively brief but powerful instruction format yielded exciting results when used in combination with high quality questioning.

In the main trial, over 150 participants taking part in teams solved a series of complex puzzles in order to 'escape' from a confined environment – a challenging Escape Room. Immediately after getting out of the room, and in an analogue of some of the real-world scenarios outlined above, all participants were interviewed separately to find out how they escaped. The challenge for interviewers was to conduct those interviews within 10 minutes. All interviews included an initial free report and follow-up questioning.

Escapees interviewed using the TCQ framework provided significantly **more** actionable information (puzzle solutions) and otherwise critical information about 'how to escape' (the purpose of the interview) than escapees who were interviewed using a direct questioning approach. This difference was apparent both after the initial free report and follow-up questioning. Closer inspection of reporting patterns also showed that a larger proportion of participants interviewed using the direct approach provided no actionable information at all in their interviews.

Recently, the TCQ framework was trialled by Counter Terrorism Police South East interviewers in a live hostage-taking scenario training exercise. Interviewers were trained in the TCQ framework and, a few days later, officers used it to interview 'hostages' who had escaped from a stronghold. Anecdotally, interviewers reported that they obtained 'huge amounts' of information using the technique although they wanted more time to practice it. Officers trained in the TCQ framework reported that, if permitted, they would use the framework in time critical incidents. Some also commented on the potential for wider application in policing, extending to any situation where officers need to quickly elicit information to assess a situation. Generally, one of the main perceived benefits of the TCQ framework commented on by practitioners to date has been that this approach provides a useful structure both for the interviewer and the interviewee for an initial interaction in high pressure contexts.

Our research provides the first empirical evidence that a carefully-structured orienting instruction focused on aligning the roles, goals, and expectations of interviewer and interviewee delivered at the outset of a brief interview can significantly and positively impact the amount of tactical information provided by an interviewee under time-critical conditions. Following these promising results, our next step is to continue to tailor and maximise the utility of the TCQ framework across a range of operational scenarios.

Lorraine Hope is Professor of Applied Cognitive Psychology at the University of Portsmouth and a Principal Investigator in CREST. Her work focuses on information elicitation, intelligence gathering, and the performance of human cognition in applied contexts, including memory and decision-making under challenging conditions.

Feni Kontogianni is a lecturer in the Department of Psychology at the University of Winchester and a Co-Investigator in CREST. Her work has focused on information elicitation, and the effectiveness of techniques that facilitate memory recall and reporting in policing and security settings.

Alejandra De La Fuente Vilar is Senior Research Associate in the Department of Psychology at the University of Portsmouth. In addition to CREST research on information elicitation in both face-to-face and online contexts, her work focuses on cooperation and overcoming reluctance in interviews.

CHARIS RICE AND MARTIN INNES

WHAT'S NEW, WHAT WORKS?
COUNTERING-TERRORISM WITH PUBLIC-FACING STRATEGIC COMMUNICATION CAMPAIGNS

How can we innovate to communicate more effectively with the public about counter-terrorism? Charis Rice and Martin Innes respond to this challenge using the 'Situational Threat and Response Signals (STARS)' research project.

Public facing strategic communication campaigns are now a mainstay in countering terrorism. Messaging campaigns have been used to encourage public reporting of suspicious behaviour, to reassure citizens, and to try and deter hostile behaviours. However, a recurring concern is that messaging about terrorism might have unintended consequences, such as boosting fear rather than reassurance. Fundamentally, 'what works' in designing and delivering effective and impactful public communications remains unclear.

The 'Situational Threat and Response Signals (STARS)' research project responds to the challenge of how to communicate effectively with the public about terrorism in an increasingly complex and fragmented information environment. Following a multidisciplinary literature review, we used frame analysis of a sample of campaigns, practitioner interviews, public focus groups, and social media analysis to examine three UK campaigns – 'See it, Say it, Sorted', 'Action Counters Terrorism', and 'Security On Your Side'. Taking a view that context is likely to matter, we captured practitioner and public perspectives across different (urban and rural) parts of the UK: England, Wales, and Northern Ireland.

IF A CAMPAIGN IS THE ANSWER, WHAT IS THE PROBLEM?

We identified two key tensions that frustrate the design and delivery of counter terrorism (CT) campaigns:

1. The 'fear trap': When CT campaigns try to 'outbid' other risks or even different types of terrorist threat, they can unintentionally create the negative emotional reactions being sought by terrorists. Equally, balancing levels of reassurance against enough fear to command public attention is challenging, particularly within those communities where terrorism or other threats are relatively 'normal'.
2. The 'fame trap': Comes from creating 'too much' awareness of terrorism in the general population, often driven by using commercial marketing logics to try to get attention and cut through in the crowded information environment. Moreover, the public are probably most receptive to CT messaging in the aftermath of 'signal events', when it is actually required less; and accessing the right audience segments while not diluting the core message involves seeking a 'Goldilocks moment' that is 'just right'.

> *"The problem is that a lot of the people that are developing these campaigns are also living in those nicely middle-class suburbs and don't have the lived experience, don't know how this is going to land. So a lot of working effort needs to go into actually thinking through the audiences that we're trying to speak to... their experiences... whether they are aware that they're even being affected by this"* (Practitioner, Northern Ireland).

A USER-LED APPROACH: WHAT WOULD THIS LOOK LIKE?

Most practitioners were very focused on how to harness social media for campaign effectiveness. However, we found little day-to-day public engagement with campaign hashtags on Twitter. The overall picture was of police and partner agency related accounts, posting and reposting one another, but capturing little public attention.

Concurrently, in our focus groups and interviews across the UK, we captured insights on what a 'user-led' campaign would involve and problems with current public engagement approaches. Five key themes emerged.

PROBLEMS: Public trust is a critical problem for CT, and there is a tentative awareness among practitioners that tackling distrust requires a different set of objectives and measures to that of building trust (Rice *et al*., 2021). A related problem concerns how resonant current campaigns are with lived experience.

PEOPLE: Speaking to both of these issues, practitioners discussed direct, face to face public engagement as critical to public trust building. This can be done via local police patrols and interactions with the public, and specifically Project Servator deployments, as well as outsourcing communication to "community messengers" (P15, England). Community messengers may be helpful both for widening dissemination, but also because citizens and community leaders are able to message and engage in boundary pushing ways, for example through humour and satire, where it would not be appropriate for governments to try and replicate.

PLACES: Making a message persuasive and impactful can be accomplished by innovating through the mediums and the delivery spaces, as much as message content. In addition to the social media arena, practitioners saw promise in cost-effective localised delivery measures via local authorities and councils, local business forums, or community organisations.

When discussing the right places and mediums for CT public facing campaigns in the focus groups, participants mentioned traditional methods such as television and radio adverts, schools based initiatives and face to face education, in addition to online (social) media avenues. Examples were given of health promotion communication campaigns in this respect and initiatives such as the green cross code.

PRODUCTS: Relatedly, product suggestions included physical assets such as messages on train tickets or posters inside public toilet doors (similar to the 'Ask Angela' notices) and 'token' marketing such as key rings. This reflects the approach of community 'nudges' and 'ritual models' that have proved successful in other contexts such as natural disaster preparation (Heath *et al*., 2017).

POSSIBILITIES: Commercial techniques and new technologies present new possibilities for improving campaign pre-testing and evaluation (e.g., testing emotional responses through facial recognition software) rather than solely to the transmission of campaign messaging. The power of narrative and storytelling was considered by several practitioners to be an under-used technique in the CT space, underpinning to some extent the reasons why community messengers were considered effective.

> *"It [the Green Cross Code campaign] worked because they came around the school and they asked questions and the children got involved, and you had a little badge and things, but you know, I'm talking about 60 years ago, and I can still remember those"* (Urban, Male, 66, White, Cardiff).

WHAT'S NEW, WHAT WORKS? ADAPTATION VS INNOVATION

These findings have implications for the view of innovation in counter-terrorism public-facing communication. Rather than innovation being viewed as a chase to keep up with the fast paced social media trajectory, it may be better considered as adapting messaging to particular situations, which may or may not require 'new' methods. Part of this adaptation may be translating issues into their local context through established community relationships and traditional mediums, using narrative techniques to engage audiences and explain messaging rationale.

To this end, the *'STARS' framework* provides a structured approach that those constructing CT campaigns can work through to help focus their communications to deliver targeted impact.

Charis Rice is an assistant professor at Coventry University. Her research focuses on strategic communication, security, and trust.

Martin Innes is a professor at Cardiff University, where he is Co-Director of the Security, Crime and Intelligence Innovation Institute. His work on policing, counter-terrorism and disinformation has been internationally influential across the academic, policy and practice communities.

LUCY MASON

IS 'GOVERNMENT' AND 'INNOVATION' AN OXYMORON? PUBLIC SECTOR INNOVATION: A PRACTITIONER'S PERSPECTIVE

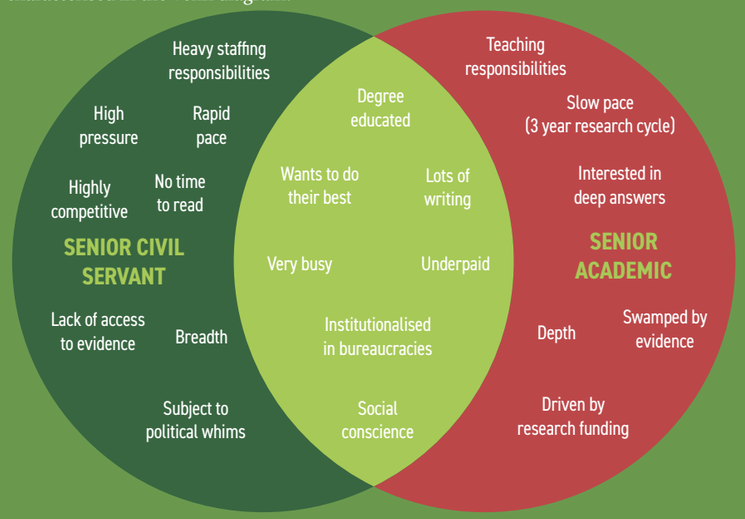
Civil servants and academics need to talk to each other more, in language each understand, to help research and evidence better inform public sector policy – especially in security.

THE PROBLEM

Public sector innovation is needed to tackle the big challenges we face as a society – how to keep people safe, protect the vulnerable, and create a fair and just world in an ever-changing socio-techno-political-geographic context. It relies on the 'triple helix' of industry, academia and government working together to create solutions. All too often, innovation fails because of poor inter-relationships between different stakeholders – in this case, we are focusing on civil servants and academics. This article argues that better mutual understanding and adapting accordingly would improve the translation of research and evidence into innovative public policy – ultimately, making a positive difference for us all.

Civil servants and academics have considerable overlap in the types of people who choose those careers – usually degree-educated, and with a passion for doing good in the world (social conscience) which has deterred them from seeking greater riches in industry. But the career pathways in each sector funnel people into ways of thinking and acting, certainly by the time people have reached senior roles – which can lead to a communication and cultural divide – rather crudely characterised in the Venn diagram.

Without wishing to be stereotypical (for of course every institution contains a rich diversity of people and for every rule there is an exception), civil servants are often working at great pace under huge pressure, with goals constantly moving and many stakeholders with often conflicting views. They don't have the time for slow contemplation, deep reading around their policy area, or to get 'out and about' to meet and build personal networks and connections with academics. They don't read peer-reviewed academic journals, which are often hidden behind paywalls. Often generalists, they have 'breadth' rather than 'depth'. Academics do of course lead busy lives under pressure, but I would argue to a very different extent to most civil servants working in Central Government policy departments. Academics have usually chosen a field they are fascinated by and spend their time (often many years) developing and keeping current a great depth of knowledge. Obviously, accessing this knowledge benefits public policy making. And yet, despite years of Governments' promising 'evidence based' policymaking, this often fails.



Why does research and evidence fail to influence policy as it should?

In many ways civil servants and academics simply speak different languages. They operate in organisational cultures which operate with a very different pace, set of cultural norms, funding routes, priorities, and approaches. So different, in fact, as to be incompatible in some ways: a civil servant might have an afternoon, or a day, or just hours, to draft a policy paper for a minister but an academic asked for an opinion might want weeks or months to provide a properly considered and fully referenced response. A civil servant briefing to a minister needs to be succinct, clear, and helpful in offering tangible advice on what to do: an academic paper is typically densely written, highly nuanced and often using very specific (often contested) terminologies. A civil servant developing policy needs to consider not only the evidence base (often lacking for emerging policy areas, by the very nature of trying to do 'new' things) but also what interest groups want, what the public might accept, how the media might engage with the issue, and what might be uppermost in the Minister's mind. A perfectly sensible policy decision can easily be derailed by a Twitter storm that morning. In contrast academic research is much less susceptible to the ebbs and flows of public discourse and has the luxury of being more purist in its approach to what is and is not good information – but also the disbenefits of having far too much research to get to grips with.

THE SOLUTION(S)

In my career, I have taken a very people-orientated approach to public sector innovation, arguing that it is about people and culture much more than systems and processes. This lens is not often applied but offers a truly transformational approach. Behavioural science insights and human-centred research is key to this understanding – as applied effectively during the response to the COVID-19 pandemic. Based on my work across and within the civil service, academia and private sector, I'd suggest the following advice helps us focus on the people within the systems:

Civil Servants

- Remember the value academics can add in policy design and independent evaluation, and actively seek them out/ build trusted relationships with some key people
- Help inform research agendas by setting out your 'problems', challenges, and areas of interest as specifically and clearly as you can
- Remember to introduce your networks to your successors and hand off relationships as you move roles: stay in touch and update contact details so people can find you again
- Try to speak in plain English with little jargon and acronyms when engaging externally, so people can understand what you mean
- Try to be consistent over time in policy areas and plan ahead so academics can engage over longer timescales (useful research cannot be undertaken in a day)
- Invite academics in (secondments, placements, talks, workshops) to talk about their work and what it means for your policy area

Academics

- Be easy to find through a Google search and LinkedIn on keywords and with a working email address/ phone number to access you quickly if needed
- Be active in networks where civil servants might be present: try Innovate UK KTNs, TechUK, Academic RISC, CREST, SPRITE+, PETRAS and other specialist knowledge networks
- Write short informative summaries: make sure the abstract sets out the findings and 'so what?' for users (i.e., what you want them to do as a result) – see POST Notes for good examples
- Remember a busy civil servant may be less interested in the detail, and more in your advice/ recommendations especially for tangible actions which can be taken (your expertise speaks for your credibility)
- Be clear about whether a recommendation is based on clear, robust evidence/ widely agreed or whether there is considerable uncertainty/ dissent

Both sides need to spend more time talking to one another, not only about specific research topics but about their cultures, incentives, and pressures, and listening to the other. It's not simply a question of one side fitting themselves around the other: both sectors need to meet in the middle, and that means challenging some of the ways things are done now. That might mean new kinds of academic roles – ones which have time set aside to build capacity for short turnaround projects for rapid response and building a flexible national capability. It might mean new kinds of civil service roles, specifically targeting external engagement and getting value out of networking, not as a side hustle. And both need to invest seriously in a long-term strategy for training and skills development, for a diverse pipeline of talent who are recognised experts at collaboration (which is a skillset in its own right).

NEXT STEPS

Innovation is all about people. The difference between success or failure depends on what different people wake up and decide to do with their day. And especially now, when innovation requires collaboration between many different stakeholders working together as a (often virtual) team, innovation needs the right conditions to flourish. As a lifelong practitioner of public sector innovation – first as a civil servant, now as a private sector consultant – I'm convinced many of the challenges can be solved by getting people to work better together.

Dr Lucy Mason is the Director for Defence and Security Innovation in Capgemini Invent and the founder and former Head of the Defence and Security Accelerator (DASA). With 20 years' experience across policing, security and defence, Lucy has worked extensively with the academic and security communities. This article is the author's opinion and does not represent Capgemini Invent. Twitter: @DrLucyMason

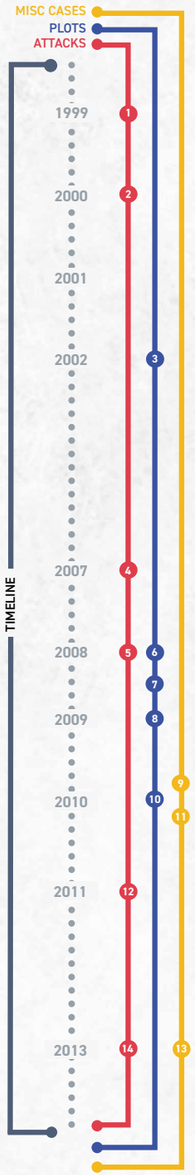
BENJAMIN LEE, DEANNA REDER & CAMERON GREIG

EXTREME RIGHT-WING TERRORISM IN THE UK

This timeline provides an overview of sentences stemming from right-wing terror attacks, plots, and offences in the UK between 1999 and summer 2022.

The timeline is intended to give some insight into the extent of offending connected to right-wing terrorism since 1999 and demonstrate the broad range of offenders, offences, and locations involved. It reflects the day-to-day reality of terrorism offending originating from the extreme-right, but also highlights how much right-wing activity may not be accounted for in this type of analysis.

Individual entries refer to sentences given and not the date of specific attacks or offences. This timeline is based on open source reporting only. Definitions of terrorist attacks and terrorist plots can vary. This should not be interpreted as a comprehensive list of right-wing terrorism or extremism. This timeline does not reflect wider harms connected to the extreme-right, such as online harassment.



1). NOV 1999: KERR
Stuart Kerr (20) sentenced to 12 years in prison after firebombing an Asian owned shop. *Mein Kampf*, and material from racist groups were found in Kerr's flat. Reported in The Evening Standard 23/11/1999.

2). JUN 2000: COPELAND
David Copeland (22) sentenced to six life sentences after killing three people in a bombing campaign focused on areas of London linked to minority groups. He remains the UK's most deadly right-wing terrorist.

3). OCT 2002: TOVEY
David Tovey sentenced to 11 years on firearms and explosives charges. The police raided Tovey's Oxfordshire home investigating a racist graffiti campaign. They found weapons, improvised explosives, a sketch map of Mosques and a list of car number plates belonging to Black and Asian families.

4). JAN 2007: BULMAN
Mark Bulman (22) sentenced to five years for arson, attempted arson and two counts of religiously aggravated damage to property. Bulman turned himself into the police after he threw a firebomb into a Swindon Mosque. The bomb failed to ignite. Bulman had previously been active with the BNP.

5). JUN 2008: AZERVEDO
Jefferson Azervedo (45) sentenced to four years for a letter campaign in which he sent white powder to targets and planting a hoax bomb under a Swastika flag on a footbridge.

6). JUN 2008: GILLEARD
Martyn Gilleard (31) sentenced to 16 years for terrorism and child pornography offences. Police found ammunition, nail bombs, and documents outlining extreme anti-Semitic views while investigating Gilleard for child pornography. Gilleard was reported to be a member of the National Front, British People's Party, the White Nationalist Party, and had modified a hi-vis jacket to reference Combat 18.

7). DEC 2008: WORRELL
Nathan Worrell (35) sentenced to seven years and three months for offences including possession of material for terrorist purposes and racially aggravated harassment. Worrell was engaged in a campaign of harassment against a mixed-race couple. Worrell was reported to have membership cards for the November Ninth Society, KKK and the British People's Party.

8). SEP 2009: LEWINGTON
Neil Lewington (44) receives an indefinite prison sentence for possession of explosives with intent to endanger life and preparing an act of terrorism.

9). JAN 2010: GAVAN
One time BNP member Terence Gavan (39) sentenced to 11 years after police uncover a massive cache of weapons and explosives. Gavan is convicted of 22 counts of firearms and explosives offences as well as six terrorism offences. Despite the size of the cache there is no information about Gavan's intentions.

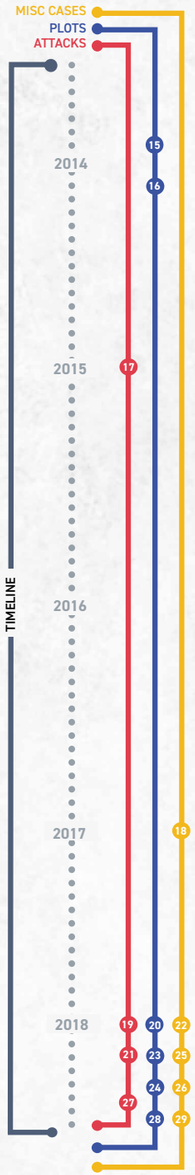
10). MAY 2010: DAVISONS
Ian Davison (41) and Nicky Davison (19) are sentenced to ten years and two years detention respectively after manufacturing ricin in their kitchen. Both are affiliated with the group Aryan Strike Force (ASF).

11). JUN 2010: HANNINGTON
Trevor Hannington (58) is sentenced to two years for two counts of stirring up racial hatred, and two counts of possessing information useful to terrorism. Hannington was an administrator for the ASF website.

12). DEC 2011: BEECH/FOSTER
Simon Beech (23) and Garreth Foster (29) each sentenced to ten years for an arson with intent to endanger life as the result of an attack on a Stoke Mosque.

13). SEP 2013: RODDY
John Roddy (20) sentenced to 23 months suspended for possession of documents useful to terrorism.

14). OCT 2013: LAPSHYN
Pavlo Lapshyn (23), a Ukrainian exchange student, sentenced to life with a minimum of 40 years for the murder of a Muslim man and a series of bombs targeting Mosques. Lapshyn was later convicted of manufacturing explosives in his prison cell.



15). MAY 2014: FORMAN
Ian Forman (42) sentenced to ten years for preparing a terrorist act. Forman drew up a list of local mosques and tested homemade explosives.

16). JUL 2014: PIGGIN
Michael Piggin (18) detained under the Mental Health Act. Piggin stockpiled explosives and weapons and planned to attack his school and a mosque.

17). SEP 2015: DAVIES
Zack Davies (26) given 14 years for the attempted murder of a Sikh man in a Mold supermarket. Davies was linked to neo-Nazi group National Action.

18). FEB 2017: CREIGHTON
Sean Creighton (45) sentenced to five years for offences including collecting information useful to terrorism. Creighton was a member of the National Front.

19). JAN 2018: ZAKROCKI
Marek Zakrocki (48) sentenced to 33 weeks already served on remand for dangerous and drunk driving. Zakrocki drove his van at the owner of a curry house after giving a 'Nazi salute' and shouting 'white power' having previously told the police he was going to kill a Muslim and that he was 'doing it for Britain'. Nazi memorabilia and flyers supporting Britain First were found in Zakrocki's possession.

20). FEB 2018: SEABROOK
Liam Seabrook (31) sentenced to eight years for threatening to attack Manchester mosques in the wake of the Manchester Arena bombing. Seabrook had a previous conviction for arson and racist graffiti and informed his probation officer of his plans. Police found homemade weaponry and washing up liquid bottles of petrol at Seabrook's home.

21). FEB 2018: OSBORNE
Darren Osborne (48) receives a life sentence with a minimum of 48 years after driving a car at a group of men outside the Muslim Welfare House in Finsbury Park, London, killing one.

22). MAR 2018: VEHVILAINEN/ DEAKIN
Mikko Vehvilainen (34) sentenced to eight years for possession of an offensive weapon and stirring up racial hatred. Vehvilainen was a serving soldier and subsequently convicted of being a member of National Action; Alexander Deakin (24) sentenced to eight years for membership of a proscribed organisation (National Action).

23). APR 2018: WARD
Connor Ward (25) sentenced to life with a minimum of six years for terrorism offences. Ward kept a list of mosques and acquired bomb-making components.

24). MAY 2018: STABLES
Ethan Stables (20) sentenced to an indefinite hospital order for preparing an act of terrorism, threats to kill and possession of explosives linked to a plan to attack a local gay pride event.

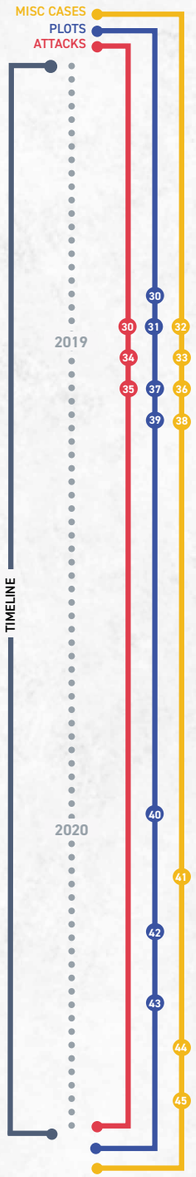
25). JUL 2018: LYTHGOE/ HANKINSON
Christopher Lythgoe (32) sentenced to eight years for membership of a proscribed organisation (National Action); Matthew Hankinson (24) sentenced to six years for membership of a proscribed organisation (National Action).

26). JUL 2018: COULSON
Jack Coulson (19) sentenced to four years and eight months in youth custody for possession of a document for terrorist purposes. Coulson had a previous conviction for making an explosive.

27). AUG 2018: ROSS
Austin Ross (23) sentenced to six years for 15 charges including two counts of arson. Ross went on a multi-day spree of criminal damage and arson including putting up a poster referencing the System Resistance Network. Ross attempted to burn down a Masonic lodge.

28). AUG 2018: MORGAN
Peter Morgan (35) sentenced to 12 years after police discover a bomb-making factory in his home along with racist material. Morgan was photograph at a rally holding a poster for the National Front.

29). DEC 2018: MULTIPLE SENTENCES
Joel Wilmore (24) sentenced to five years ten months for membership of a proscribed organisation (National Action); Adam Thomas (22) sentenced to six years six months for membership of a proscribed organisation (National Action); Claudia Patatas (38) sentenced to five years for membership of a proscribed organisation (National Action); Daniel Bogunovic (27) sentenced to six years four months for membership of a proscribed organisation (National Action); Darren Fletcher (28) sentenced to five years for membership of a proscribed organisation (National Action); Nathan Pryke (27) sentenced to five years five months for membership of a proscribed organisation (National Action).



30). APR 2019: BISHOP/FLETCHER

Steven Bishop (41) sentenced to four years for possession of explosives and possession of material useful for terrorism. Bishop planned to attack a London Mosque in revenge for the Manchester Arena bombing and had acquired explosive material. Shane Fletcher (21) sentenced to nine years for soliciting murder and possession of information useful for terrorism. Fletcher planned to attack a football match and attempted to recruit a friend.

31). MAY 2019: RENSHAW

Jack Renshaw (23) jailed for life with a minimum of 20 years for a plot to kill a Labour MP. Renshaw disclosed his plot to a group of associates, one of whom defected to Hope Not Hate. Renshaw had previously been connected to National Action. It subsequently emerged that Renshaw was also guilty of sexual offences against children.

32). JUN 2019: Multiple Sentences

Oskar Dunn-Koczorowski (18) sentenced to 18 months detention for two charges of encouraging terrorism. Dunn-Koczorowski was affiliated to Sonnenkrieg Division (SKD).; Michael Szewczuk (19) sentenced to four years for two counts of encouraging terrorism and five counts of possessing documents useful to terrorism. Szewczuk was affiliated to SKD.

33). JUL 2019: WARD

Daniel Ward (28) sentenced to three years six months for membership of a proscribed organisation (National Action).

34). JUL 2019: MORGAN

Tristan Morgan (52) sentenced to an indefinite hospital order for arson with intent to endanger life after attempting to burn down an Exeter Synagogue. Morgan was reportedly obsessed with anti-Semitic material.

35). SEP 2019: FULLER

Vincent Fuller (50) sentenced to 23 years and 10 months following a rampage that culminated in the attempted murder of a man of Bulgarian heritage. Fuller had viewed the Christchurch Livestream video prior to the attack.

36). SEP 2019: GOLASZEWSKI

Pawel Golaszewski (34) sentenced to two years two months for possessing 'terror manuals'.

37). SEP 2019: CLEARY

Kieran Cleary (16) sentenced to five years detention. Cleary acquired bomb components and told friends he planned to go on a rampage. He had earlier praised Hitler.

38). OCT 2019: DUDGEON/SEALES/LONGO

David Dudgeon (43) sentenced to two years for possessing information useful to terrorism. Morgan Seales (20) sentenced to four years for encouraging terrorism. Gabriele Longo (26) sentenced to six years for encouraging terrorism.

39). NOV 2019: REED

Jack Reed (16) - at the time the youngest person in the UK to be convicted of a terrorism offence - was sentenced to six years and eight months for terrorism offences. Reed researched explosives and drew up a hit list of potential targets in Durham. Reed was further sentenced for sexual offences.

40). MAY 2020: FOWLE

George Fowle sentenced to 20 months suspended for two counts of making a record useful for terrorism. Fowle was arrested at Heathrow Airport. He was in possession of bomb-making instructions and had announced his intention to attack Camp America, although the plot was reportedly immature.

41). JUN 2020: SCOTHERN/CUTTER/JONES/JACK

Conor Scothern (19) sentenced to 18 months in a young offenders institution for membership of a proscribed organisation (National Action). Alice Cutter (23) sentenced to three years for membership of a proscribed organisation (National Action); Mark Jones (25) sentenced to five years six months for membership of a proscribed organisation (National Action); Garry Jack (24) sentenced to four years six months for membership of a proscribed organisation (National Action).

42). JUL 2020: TCHORZEWSKI

Jacek Tchorzewski (19) sentenced to four years for ten counts of possessing information useful to terrorism, affiliated to SKD.

43). NOV 2020: DUNLEAVY/BEDNARCZYK

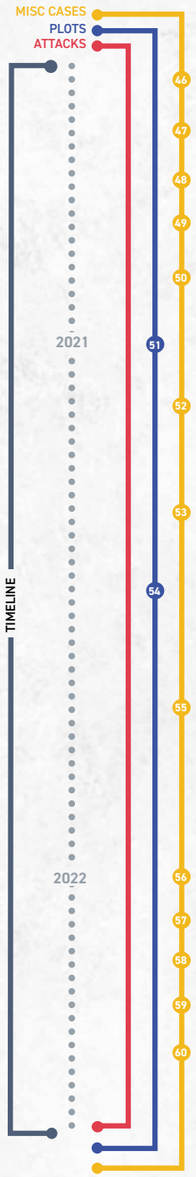
Paul Dunleavy (17) sentenced to five years and six months for a plot to 'commit an act of terrorism' but described as inept by the judge. Dunleavy was a member of FKD. Filip Golan Bednarczyk (26) sentenced to four years for seven charges of possessing a document useful for terrorism and possession of an explosive substance.

44). NOV 2020: VAUGHAN

Harry Vaughan (18) sentenced to two years suspended sentence for 12 counts of possessing documents useful to terrorism, one count of encouraging terrorism and one count of disseminating a terrorist publication.

45). DEC 2020: HUNTER

Luke Hunter (23) sentenced to four years two months for four counts of encouraging terrorism and three counts of disseminating a terrorist publication.



46). FEB 2021: UNNAMED

An unnamed 13 year-old is sentenced to a two year youth rehabilitation order for two counts of disseminating terrorist publications and ten counts of possession of documents useful to terrorism.

47). MAR 2021: UNNAMED

An unnamed 16 year-old is given a 12 month referral order for four counts of support for a proscribed organisation, three counts of encouraging terrorism, and four counts of stirring up racial hatred.

48). APR 2021: HANNAM/UNNAMED

Benjamin Hannam (22) is sentenced to four years and four months for charges including membership of a proscribed organisation (National Action). Hannam was a probationary officer in the Met. An unnamed 16 year-old is given a 12 month referral order for a series of charges including possessing documents useful to terrorism.

49). MAY 2021: GREGORY/NIMMO/BEL/BROCK

Robert Gregory (24) sentenced to four years six months for accessing information useful to terrorism. John Nimmo (32) sentenced to ten years two months for a series of offences including possessing a prohibited firearm and distributing a terrorist publication. Oliver Bel (24) sentenced to two years for possessing information useful to terrorism. Nicholas Brock (53) sentenced to four years for possessing material that could be used to prepare terrorist acts.

50). JUN 2021: NUGENT

Michael Nugent (38) sentenced to five years for five counts of disseminating terrorist publications and 11 counts of possessing information useful to terrorism.

51). JUN 2021: MORRICE

Dean Morrice sentenced to 18 years for possession of explosives and multiple terrorism offences. Morrice ran a neo-Nazi Telegram channel and was found in possession of bomb-making materials.

52). JUL 2021: DYMOCK/UNNAMED

Andrew Dymock (24) sentenced to seven years with a further three years on license for a string of terrorism and hate offences. Dymock was formerly a member of SRN and founded SKD. An unnamed 17 year-old is given a 12 month referral order for 11 counts of collecting material useful to terrorism.

53). SEP 2021: JOHN/UNNAMED

Ben John sentenced to two years for possessing information useful to terrorism. John's original sentence was to read classic literature but he was jailed on appeal. An unnamed 16 year-old is given a 12 month referral order for disseminating a terrorist publication. At the age of 14 this actor ran the Telegram Group The British Hand. An unnamed 16 year-old is given a two year referral order for disseminating a terrorist publication and encouraging terrorism.

54). OCT 2021: CRONJAGER

Matthew Cronjager (18) sentenced to 11 years and four months for offences including preparing an act of terrorism. Cronjager was planning to murder his non-white friend using a 3D printed firearm.

55). DEC 2021: IMRIE/RAYMOND

Sam Imrie (24) is jailed for seven years and six months for several offences including two terrorism offences. Ben Raymond (32) is jailed for eight years for membership of a proscribed group and possession of documents useful to terrorism. Raymond was co-founder of National Action.

56). FEB 2022: BURKE/HOWARTH

Connor Burke (19) is sentenced to three years and six months for one count of disseminating a terrorist publication and four counts of possessing documents useful to terrorism. Conrad Howarth (41) is sentenced to four years and six months for possessing documents useful to terrorism.

57). MAR 2022: UNNAMED/HENEGAN

An unknown 16 year-old is given a 12 month referral order for terrorism offences. Matthew Henegan (36) sentenced to eight years and one month for possession of a document useful to terrorism as well as a string of racial hatred offences.

58). APR 2022: LEECH

Thomas Leech (19) is sentenced to two years for one count of encouraging terrorism and other hate offences.

59). MAY 2022: MUSINS

David Musins (36) sentenced to three years for membership of a proscribed group (National Action).

60). JUN 2022: DAVIES/WRIGHT/WHIBLEY

Alex Davies (27) is sentenced to eight years and six months for membership of a proscribed organisation. Davies co-founded National Action. Daniel Wright (30) and Samuel Whibley (29) sentenced to 12 years and 10 years respectively for terrorism offences as part of the 'Oaken Hearth' cell. The group shared right-wing texts, guides for making explosives, and was attempting to make 3D printed firearms. Other members are convicted of firearms charges.

For a fuller discussion of the limitations of this timeline and definitional issues, refer to the detailed report on the CREST website, which includes an interactive version of the timeline: www.crestresearch.ac.uk/resources/timeline-extreme-right-wing-terrorism-in-the-uk/

Dr Benjamin Lee is a senior research associate at the Centre for the Study of Terrorism and Political Violence at the University of St Andrews where he focuses on terrorism and the transnational extreme-right. Deanna Reder is a 2023 MPhil candidate for St Andrews' Peacebuilding and Mediation programme. Her interests are women, peace, and security (WPS), women in extremist sub-cultures, and how non-combatants respond to extremism. Cameron Greig is an undergraduate student in the School of International Relations at the University of St Andrews. His research interests relate to the extreme-right, the politics of the internet, and legitimacy.

SUSAN STEEN

A COMMUNICATION PERSPECTIVE ON RESILIENCE

A communication perspective offers an important framework for understanding resilience, especially within military cultural contexts.

Military members, along with security forces and first responders, face pressures and demands in their work that are nearly unparalleled in other professions and that may threaten or undermine their resilience. Amid growing mental and behavioral health concerns and a continued rise in deaths by suicide among active-duty military members, the US Department of Defense and various service branches have launched a myriad of initiatives designed to cultivate and strengthen resilience, defined as the ability to withstand, recover and grow in the face of stressors and changing demands (CJCSI 3405.1, 2011), across the forces.

While much of the effort within the military has historically centered on personal resilience, a task force I lead at Air University, sponsored by the Air Force Office of Resilience, has recently expanded the focus to include key perspectives, approaches, and theories of resilience from a range of academic fields and to examine individual, social, and organisational dimensions of resilience. The task force includes faculty and students who engage in a year-long project to identify best practices for creating cultures of resilience and community across the Air Force, military and DOD. Resilience speaks to the health and well-being of individuals, organisations, and communities; to their capacity to maintain core purpose, adapt, and perhaps even thrive in the wake of adversity.

Not something that only some people 'have' while others do not, nor something we generate solely and continuously on our own (Buzzanell, 2018), resilience is enacted in and through mindful practices, communication and social connection that enhance our ability to carry on and,in the military context, achieve mission goals, in the face of disruption, loss, or disaster.

THE UTILITY OF A COMMUNICATION PERSPECTIVE

In recent decades, important advances across a variety of scholarly disciplines have emerged to guide the study, teaching, and practice of resilience. Within the burgeoning field of resilience work, one approach that may hold particular promise is a communication perspective on resilience. A communication perspective considers communication an essential force in defining social reality, focusing on both the *processes* and *effects* of communicative messages. It suggests that communication shapes how we engage in meaning-making, forge and maintain relationships, create shared practices, negotiate social reality, and understand ourselves in relation to others. This perspective offers frameworks for understanding resilience that differ from the clinical or social psychological approaches that are also included in our group's examination, drawing upon theories that emphasise the socially constructed nature of sensemaking and that underscore the importance of cultivating healthy communication practices in managing multi-faceted and unpredictable interaction, especially following disruption or catastrophe. Below I offer a brief description of three communication theories that offer significant contributions to understanding and developing resilience.

The Theory of Resilience & Relational Load (TRRL) was developed by Afifi, Merrill, & Davis (2016) to explain and predict why some people, families and groups demonstrate resilience in the face of adversity while others do not. The theory is informed by two basic principles: that people are social beings who need to feel connection to others, and that individuals' stress trajectories are affected by those with whom they share a relationship. TRRL explores the role of relationship maintenance as essential to managing stress and strengthening resilience, and examines communication patterns that both reflect and affect stress, personal and relational health, and resilience. The theory suggests that although individuals may experience chronic stress, continuous investment in relationships in specific identified ways can help mitigate the effects of this stress and, importantly, that these strategies can be learned and developed. In studies involving close relationships, the theory has demonstrated that communal orientation and reserves of 'emotional capital' serve to strengthen resilience before, during and after disruptions occur. While it has been tested largely in families and romantic partnerships, TRRL holds promise for application to other kinds of close relationships, including the intensely communal bonds typically shared by military members.

The Communication Theory of Resilience (CTR), Buzzanell (2010, 2018) situates resilience in human interaction, drawing upon processes that involve multilayered systems of adaptation and transformation over time. CTR argues that resilience involves five key communicative processes that individuals and groups use to foster productive change after adversity and seeks to explain how people employ discursive and material resources to create a 'new normal' after loss, trauma or disruption. These processes include crafting normalcy, through interaction, rituals and story-telling, e.g., deliberately focusing on productive action while backgrounding negative feelings; affirming identity anchors (the ways individuals describe themselves in relation to others); maintaining and utilising communication networks for support; and developing alternative logics (in a sense, reframing) to make sense of, and adapt to, radically changed circumstances. The theory, which emerged from research involving a variety of contexts including job loss, military deployment in families, loss of loved ones, and chronic illness, offers pragmatic ways to understand and leverage communication and social connection in strengthening resilience among families, groups, organisations, and communities.

Often described as a practical theory with a critical edge, **the Coordinated Management of Meaning (CMM) Theory**, proposed by Barnett Pearce and Vern Cronen (1980), focuses on resources and practices that people can cultivate to construct and engage healthy patterns of communication in an attempt to create better social worlds. As described by Robyn Penman (2014): "CMM theory is premised on what is called a *communication perspective* that orients the practitioner or researcher to look directly at the patterns of communicating, rather than looking through communication to its outcomes." The Cosmopolitan Communication model (Pearce, 1989), deriving from CMM, offers approaches and strategies designed to engage difference and bridge gaps in culture and communication in order to achieve effective interaction among diverse people and groups. Cosmopolitan Communication both requires and enhances the capacity for perspective-taking, thereby equipping individuals and groups with tools to create space for shared understandings, if not always agreement or approval, within interaction and relationships. The model holds particular promise for the US military given its ethnic, gender and religious diversity, among other dimensions. Deliberate and mindful effort is required to leverage these differences while establishing common purpose in building effective teams (Whitt & Steen, 2021) – an indispensable part of military readiness (Goodwin, Blacksmith & Coats, 2018).

EMERGENT FINDINGS

As our 'deep dive' into the important subject of resilience has progressed, some notable conclusions have emerged. One is that, like adversity, resilience is not one-size-fits-all and rarely occurs along a linear trajectory; people may respond very differently to the same traumatic events, with sense-making and appraisal playing key roles in the process. Another is that resilience is not a 'one-and-done' outcome but a process that develops over time, drawing continuously upon resources, practices and skills derived through and after loss, disruption, trauma, or disaster. We have learned that social connection plays a compelling role and, given the nature of military culture with its strong collective identity and orientation, this may offer exponential benefits in enhancing resilience within military groups. Finally, we understand resilience in groups, organisations and communities as not simply the result of having resilient individuals within them, but as something more – an interactive effect of people, environment, context, relationships, processes, and structures. Yes indeed, the whole is greater than the sum of its parts. A communication perspective offers a distinctive lens for understanding the interaction of these processes, and for leveraging the important role of social connection, in creating cultures that foster, encourage, and nourish resilience.

Susan Steen, Ph.D. is Associate Professor of Cross-Cultural Communication in the US Air Force Culture and Language Center. She is chair of the AFCLC Culture and Region department and leads the Air University Resilience Research Task Force.

The opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the views of the Air University, the United States Air Force, the Department of Defense, or any other US government agency.

LEWYS BRACE

THE 'INCELOSPHERE' AND INCEL VIOLENCE: A WORSENING PROBLEM?

Should incel ideology be considered as extremist? Lewys Brace summarises the research on how violent extremist language has increased over time as different online platforms have emerged and shutdown within the incel online ecosystem.

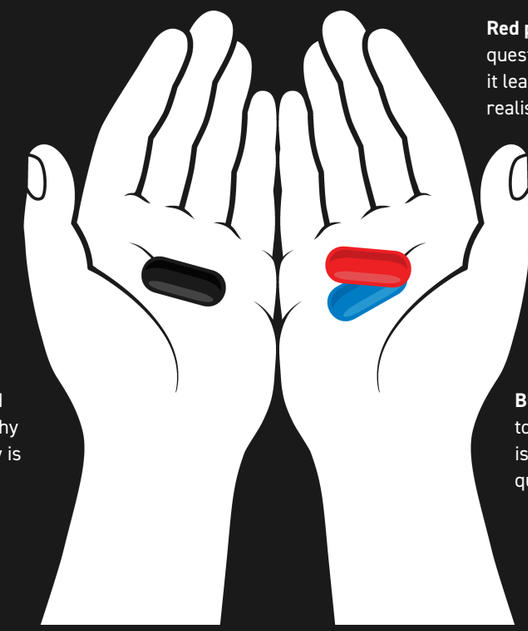
At around 1800 local time on 12th August 2021, a man carried out a spree killing in Plymouth, UK, that resulted in the deaths of five people, before ultimately taking his own life. The perpetrator, Jake Davison, was an active member in online spaces hosting incel content. In 2020, two UK teenagers who also engaged with the online incel community to some degree, faced trial for possessing terrorism-related materials.

Inevitably, these and other cases have sparked discussions in the UK regarding whether the incel ideology should be considered an extremist one, and whether those who are motived by its ideas to carry out acts of violence should be considered terrorists. The UK is not alone in this debate; Canada, for instance, listed Inceldom as a violent extremist ideology in 2019. The existence of these discussions is testament to the way in which the incel subculture and worldview is amorphous in nature, which makes it hard for researchers and practitioners to frame this worldview, and those who subscribe to it, in the traditional language of terrorism and counter-terrorism. The issue is exacerbated by the way in which ideas that are now associated with the 'incel' label have motived other forms of violence that do not constitute an act of mass-violence. For instance, a series of stabbings in Portsmouth, UK, in June-July 2014 resulted in the serious injury of three women, with the perpetrator stating in a letter to the police that "I am still a virgin, everyone is losing it before me, that's why you are my chosen target.", and further notes including misogynistic language and detailing a perceived need for revenge against women for his lack of sexual relationships.

AN EXTREMIST IDEOLOGY?

Most researchers analysing incel online communities agree that discussions taking place on these digital spaces contain highly problematic language. Some studies have argued that the incel subculture exhibits all of the characteristics of an extremist ideology (Baele, Brace & Coan, 2019; Jaki *et al*., 2019), structured by an opposition between an in-group and harmful out-group(s), with intergroup competition being presented in the form of a crisis-solution narrative (see Berger, 2018a, 2018b). It has been shown that the incel in-group/out-group(s) crisis narrative consists of a three-tiered hierarchy, where a minority of 'Alpha' males ('Chads') and females ('Stacys') stand on top, a majority of average-looking 'Betas' ('normies') follow, and a minority exclusively male and unattractive incels are stuck at the bottom, constantly oppressed and victims of relentless discrimination and harassment. The out-groups are discussed in relation to perceived negative traits, such as women being only capable of simple emotions (chiefly sexual desire) and having the tendency to cheat on their partners and manipulate men for sex or money. This three-tier hierarchy highlights the contradictory nature of the incel worldview, in that it places the incels themselves at the bottom of this social hierarchy and argues that they are oppressed by women who withhold sex from them, whilst also arguing that incels are superior to the out-groups due to their perceived intellectual superiority; what they refer to as 'high IQ' (van Brunt & Taylor, 2021). The 'black pill' concept asserts that this hierarchy not only exists, but that its categories – and ensuing discrimination against incels – are so immutable that nothing can be done to move from one social category to another; i.e., to move from being an incel to a 'normie' (Ging, 2019; Hoffman, Ware & Shapiro, 2020). The black pill concept is often discussed in relation to suicide within incel online spaces due to the extreme nihilism associated with it. Due to narratives such as this, some researchers have shown that incel spaces have similar levels of 'toxicity of discussion' as far-right platforms (Ribeiro *et al*., 2020).

> **The black pill concept is often discussed in relation to suicide within incel online spaces due to the extreme nihilism associated with it.**



Yet recent studies have highlighted that not all incels condone violence (Moskalenko *et al*., 2022), and that a lot of incel content exhibits typical anxieties of young men transitioning to adults (O'Malley, Holt & Holt, 2020). We also know that discussions in radical online communities are usually driven by a small minority of influential contributors (Scrivens *et al*., 2021; Baele *et al*., 2022), and that extremist online ecosystems are usually heterogenous in the views they host. As a result, any diagnosis of incel 'extremism' and its link with offline violence ought to rest on a detailed and multifaceted assessment of the whole community and be attuned to variations across time and individuals.

TOWARDS A NUANCED ASSESSMENT

To gain such a nuanced assessment, it is fruitful to adopt an 'ecosystem' approach to studying extremist online spaces (Baele, Brace & Coan, 2020; Hutchinson *et al*., 2022). From that perspective, the online spaces hosting incel content – such as sub-Reddits, forums, Telegram channels, or Instagram accounts – ought to be understood together as a dynamic network of interacting units, and can be collectively referred to as the 'incelosphere'. A study using computational methods to both collect and analyse all text data, and accompanying metadata 33 different online spaces (covering the period 2013-2022, yielding a dataset consisting of 11,717,516 posts) allowed for an evaluation of how extreme the content and discussions on these platforms have been over time. To evaluate the proportion of violent language in this content, we used a custom 'dictionary' or lexicon, named the 'Incel Violent Extremism Dictionary' (IVED), containing three types of words found in the corpus; dehumanising out-group nouns, violent verbs, and nouns related to weapons (Baele, Brace & Ging, 2023).

This analysis revealed that the incelosphere is not homogenous in terms of the amount of violent extremist language that features on each of the online spaces. The dedicated incel forums indeed host a greater proportion of extreme and violent words than sub-Reddits and chan boards (*figure 1*). However, at the same time, the analysis also demonstrated a worrying trend: there is a clear temporal evolution whereby, not only did the early three major incel online space (the sub-Reddits r/Incel, r/Incels, and r/Braincels) get progressively more extreme in their conversations over time, but this growing intensification of extremist language continues to this day at the ecosystem-level, with the main incel forum, Incels.is, demonstrating the highest ratios of violent language to date (*figure 2*). This is coupled with an analysis of the number of daily posts made to each online space, which demonstrated that Incels.is has also been acting as the long-standing centre point of the incelosphere since the closure of r/Braincels.

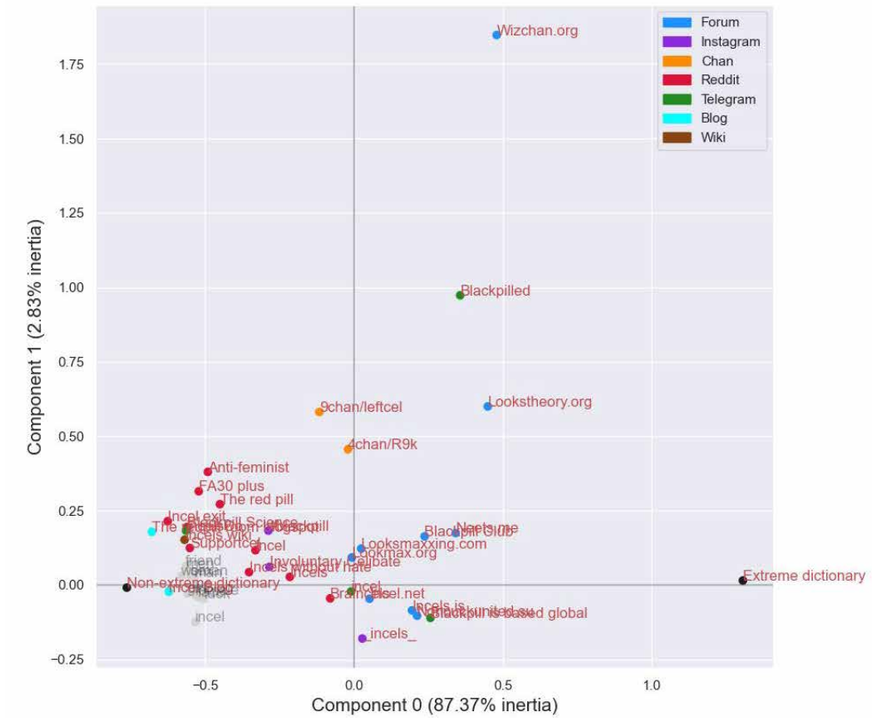


Figure 1: *Correspondence analysis of incel online spaces' lexical proximity with violent extremist language (IVED) and most common incel words. From Baele, Brace & Ging (2023).*

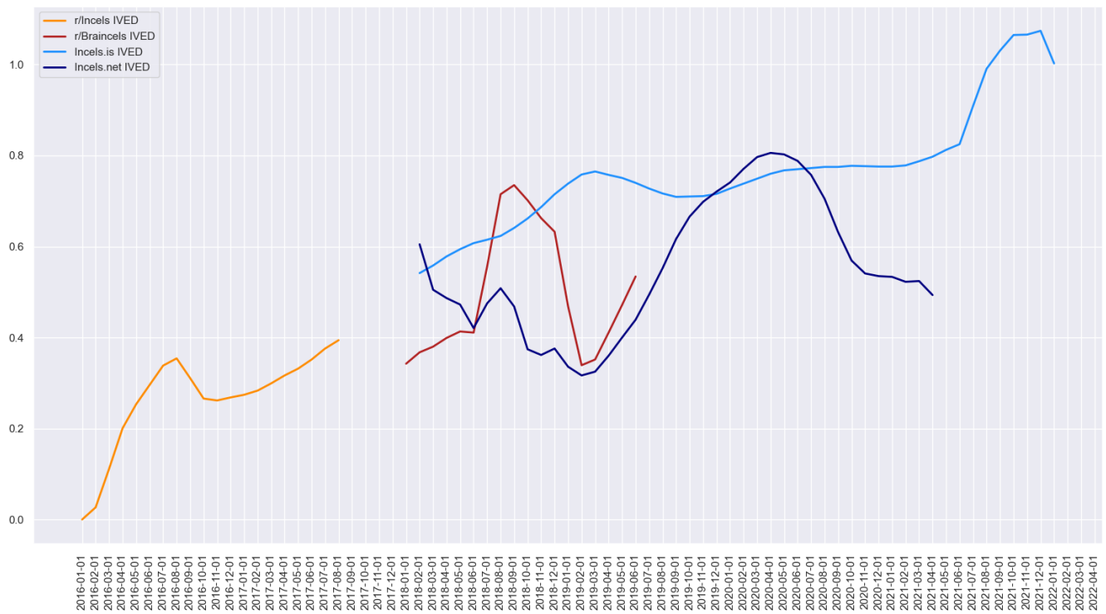


Figure 2: *Time series trend data for /r/Incels, /r/Braincels, Incels.is, and Incels.net, plotted as a 3-month rolling average. From Baele, Brace & Ging (2023).*

While empirical evidence has shown that the incel community mostly does not view acts of incel-inspired violence as a way of bringing around some form of social-political change, but instead view such acts as a form of personal revenge or cathartic release for the perpetrator (Baele, Brace & Coan, 2019; Brace, 2021), it is theoretically possible that the incel tendency towards mass violence could be conceptualised as a red pill-to-black pill pipeline. Given what is known about the demographics of the userbase (Sugiura, 2021; Williams *et al.*, 2021), it is possible that some of the younger individuals (i.e., 12-13) are engaging with this content but naturally disengaging from it as they gain life experience, resulting in their time on these online spaces being a temporary phase. However, those who do not form meaningful social relationships and instead continue to interpret their offline, real-world, experiences through the black pill ideology develop increasingly nihilistic views as they progress throughout their teenage years, which combined with the aspects of ideology described above, could increase their tendency towards violence and suicidal ideation. This might explain why a sense of hopelessness and suicidal ideation have been noted in most incel attackers (van Brunt & Taylor, 2021; Williams *et al.*, 2021) and why so many of them either commit suicide at the end of their attack or attempt 'suicide by cop'.

However, such psychological traits alone would not be sufficient in themselves to motivate an individual to carry out an act of mass violence, with research indicating that they need to be accompanied by the kind of over-generalisations, victim dehumanisation and neutralisation, and justifications seen in the incel ideology (van Brunt & Taylor, 2021; Williams *et al.*, 2021; Broyd *et al.*, 2022). Given the purely online nature of the incel subculture, it therefore becomes crucial to understand the nature of incel online spaces in relation to extremist discussions. We have seen here that the incelosphere's violent and extremist language is not homogenous and that it has increased over time. Future work should therefore focus on understanding these changes in online discussions on the incelsophere within the context of how individuals might use them as a lens through which to perceive their real-world, offline, interactions; a concept that scholars refer to as 'onlife' (Valentini, Lorusso, & Stephan, 2020).

> **...the incel tendency towards mass violence could be conceptualised as a red pill-to-black pill pipeline.**

SUMMARY

Much work remains to be done in developing an understanding of incels and the tendency towards violence. While the sample size of known incel attackers is currently, and fortunately, still quite small, analysis of their behaviours and psychological traits combined with the kind of data-driven work summarised here indicates the need to develop a nuanced understanding of the relationship between online discussion and offline push and pull factors as a motivator towards violence.

The full analysis that is summarised above can be found in Baele, S., Brace, L., & Ging, D. (2023) A Diachronic Cross-Platforms Analysis of Violent Extremist Language in the Incel Online Ecosystem, *Terrorism and Political Violence,* DOI:10.1080/09546553.2022.2161373.

This work was supported by the Economic and Social Research Council under Grant ES/V002775/1.

Dr Lewys Brace is a senior lecturer in computational social science at the University of Exeter, where he specialises in extremism, terrorism, cybercrime, and data science. His work has appeared in journals such as Terrorism and Political Violence, Behavioural Sciences of Terrorism and Political Aggression, Studies in Conflict & Terrorism, *and* Perspectives on Terrorism.

ALEXANDRA PHELAN, JESSICA WHITE, JAMES PATERSON & CLAUDIA WALLNER

MISOGYNY AND MASCULINITY:

TOWARD A TYPOLOGY OF GENDERED NARRATIVES AMONGST THE FAR-RIGHT

Misogynistic discourses and gendered narratives are prevalent amongst far-right groups in both the UK and Australia and can serve as particular drivers of radicalisation to violence.

The gendered narratives of the far-right can be directed towards all individuals, both within the movement and society at large. These narratives position individuals within a gender order, thus establishing gender power relations. They can be used to recruit, radicalise and sustain the participation of recruits, while also clearly delineating target outgroups. Expectations of masculinity are used to define the role of the ideal male, while misogyny and hostile beliefs towards women and LGBTQ+ are often justified and legitimised as part of these groups' overall ideological frameworks. Consequently, understanding the gendered norms and ideology that underpin far-right narratives across online and offline spaces can be important for understanding some drivers of radicalisation and modes of participation.

To help navigate gendered language within radicalising discourse, our team undertook a review of published propaganda, far-right extremist posts, and secondary analyses. We conceptualised the following categories and defined the typologies found within them (note that many of the narratives overlap the categories).

These typologies may assist policy makers and practitioners 1) in their conceptual understanding of the diverse 'ecosystem' of far right gendered narratives and 2) by providing potential touch points for interventions when these narratives are of concern in radicalised individuals.

> **Understanding the gendered norms and ideology that underpin far-right narratives across the online and offline sites can be important for understanding some drivers of radicalisation.**

HEGEMONIC MASCULINITY

Hegemonic masculinity refers to a structure of gender ideology and power relations that is designed to reproduce male domination and the subordination of women. It is closely linked to 'male supremacy', which is regarded as a hateful ideology that overtly advocates for the subjugation of women and the maintenance of rigid, stereotypical gender roles (i.e., 'tradwife', etc.).

A. **Female control:** this signifies gendered power relations reinforcing the control of women, including how women should behave within society and the policing of this, under the assumption that they are subordinate to men. This type is closely associated with 'male supremacy', in that women are perceived as genetically and naturally inferior to men, and their subordination is necessary for the survival of 'the white race'. For example, a far-right leader in Australia argued on a Telegram channel that women 'will never stop until you put them in their place…Put a foot down early and explain your principles or forever be a cuck.' In some cases, this type can signify the legitimisation and justification of sexual violence and rape against women as not only a means of control, but of punishment for women. In this case, the use of misogyny is sometimes intertwined with the idea of existential threats to the white race and often, but not always, directed towards women identified as being involved in interracial relationships or being deemed as race traitors. .

B. **Female compliance:** this signifies gender norms that can be framed by the group's ideology that reinforce the compliance of women, including to traditional gender roles, their roles as mothers and homemakers etc., in pursuit of the group's overall ideological objectives. For instance, chats linked to the far-right often include images of pregnant women and 'loving mothers,' and where women are seen as deviating from these appropriate societal roles their activities are seen as contributing to 'the destruction of the ethno-cultural identity of the nation'.

C. **Anti-feminism:** this signifies a backlash to gender equality and even the promotion of gender inequality, specifically opposing feminism and proposals to enhance women's or LGBTQ+ rights. This could include discourse relating to anti-abortion, birth control, women's rights to vote, women's positions as leaders, and general feminist affirmative action. Moreover, the promotion of aspects such as feminism, abortion rights, and divorce are noted as aspects that lead to the destruction of a race without 'killing it directly' while other chats outline a critique of feminism as manipulating people into 'forgetting their natural instincts' (i.e., traditional gender roles).

HYPER-MASCULINITY

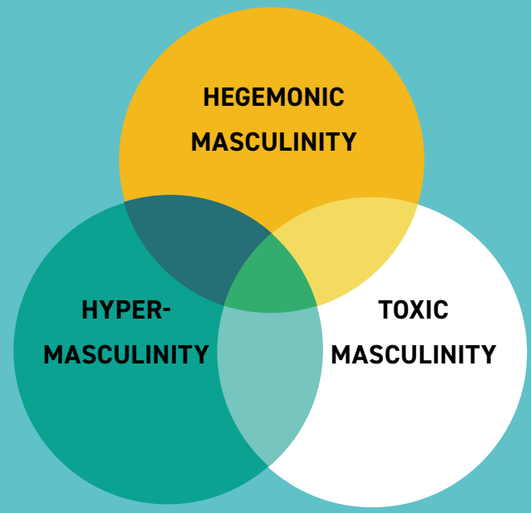
Hyper-masculinity refers to the exaggeration of masculinity and masculine stereotypes. It emphasises and reinforces 'masculine ideals and traits' that males should hold or strive towards, particularly in relation to physical strength, aggression, and dominance.

A. **The patriot 'hero':** this signifies men's specific role and duties as 'protector' and 'guardian' of the groups in pursuit of the movements' overall objectives, which could include giving up personal freedom (i.e., arrest) or safety. For example, this would relate to men fulfilling the role of 'protector' and 'guardian' of the family and racial purity, in pursuit of the 'White Nation'. It can also extend to justifying violence in the need to 'protect white daughters from dangerous animals' (non-white or non-Christian men). Passivity, in other words the absence of violence and male protection in the face of this threat, "is not an option that White people will be given if they want to survive in the future."

B. **Appeals to hyper-masculine 'brothers-in-arms':** this signifies compatriotism within the movement against non-whites, the LGBTQ+ communities, and feminists. It also includes calls that the group should 'do something' about the perceived societal discrimination against and hatred of men (allegedly promoted by feminists) in fraternal solidarity. This also extends to the targeting of other religious and ethnic groups, and the LGBTQ+ community, where anyone who is not straight (particularly transgender), white (particularly black or Muslim men), or a man (particularly committed feminists) is regarded as part of the targeted enemy outgroup and deemed a threat to the white race. The presence of these elements of society, for some far-right groups, are seen as a manifestation of a degenerate society. The perceived degeneration of these external groups are extolled to such an extent that their existence will lead to weak willed men that will not be able to stand up to the threats faced by the 'White Race.'

TOXIC MASCULINITY

Toxic masculinity refers to cultural and societal pressures for men to behave and act in certain ways that can simultaneously be harmful for men, women and the community at large. It promotes the idea that violence and acts of aggression carried out by men are the way that gender power relations and patriarchy are upheld. It can also lead to intolerance, aggressive and competitive behaviour.



A. **Male dominance:** this signifies those who embrace the idea that females are 'privileged' over men, and that men and their rights are 'oppressed' as a result. For example, movements such as the Men's Rights Movement argue that, in general, society and even institutions adversely impact and discriminate against men and boys. These movements reinforce the righteousness of male dominance, which can also extend to the legitimisation of gender-based and sexual violence.

B. **The 'ideal man':** this signifies physical masculine attributes and characteristics that men should have to participate in the movement and the rationale for this appearance, including (in some movements) the necessity for physical strength. This includes far-right groups setting up dedicated fitness chats on platforms such as Telegram and hosting regular in-person training sessions to promote and encourage 'activists and supporters to self-improve and explore our beautiful homeland'. Furthermore, one of the criteria of being a 'top tier male/female' is to 'stay in shape.' An assumption that is often promoted and overlaid onto this is the idea that white straight men are the core of white civilisation.

Dr Alexandra Phelan is a lecturer in politics and international relations at Monash University. Her expertise encompasses gendered approaches to understanding violent extremism and gendered online-messaging. Dr Jessica White is a senior research fellow in RUSI's Terrorism and Conflict research group. Her expertise encompasses CT and CVE methods, as well as gender mainstreaming in program design, implementation, and evaluation. James Paterson is a PhD candidate with the School of Social Sciences at Monash University. His research focuses conflict and security dynamics, with a particular emphasis on non-state actors and Islamist extremism. Claudia Wallner is a research fellow in RUSI's Terrorism and Conflict research group specialising in CVE, with a focus on far-right extremism.

CAMILLA DE CAMARGO

WHEN THE UNIFORM DOESN'T FIT

Innovative solutions to ill-fitting police uniforms are urgently needed (again). Dr Camilla De Camargo discusses the social, physical and mental health and safety repercussions of the current 'unisex' police uniform.

Working collaboratively with officers, academics, and designers, Camilla aims to produce a practical, comfortable, and inclusive conceptual design for all front-line police officers. This is key in supporting a police service that aims to recruit 20,000 new officers by 2025, while improving the diversity of its staff.

INTRODUCTION

For centuries, gender has been segregated by uniform at school and in the workplace, and despite some significant progress, it often still is. Various industries have faced criticism for having sexist uniform policies and demonstrated reluctance to modify outdated regulations, and every so often one of these policies, steeped in inequality, grabs the media's attention, causes controversy, and (sometimes) incites a change. There are many industries that still unwittingly embed gendered discrimination through their clothes and the design of their equipment in the workplace. A prime example of this can be found in police uniforms. Although there are psycho-social reasons why women's police uniforms need to be redesigned (including feelings of well-being and belonging), there is also evidence to suggest that wearing ill-fitting uniforms and personal protective equipment (PPE) can be extremely hazardous to health. Some progression has been seen in some arenas (tennis players/ footballers not having to wear white shorts over menstruation concerns for instance), but the police seem reluctant to make meaningful change. Why?

FITTING IN(TO UNIFORMS)

Clothing has always been a key component in the judgement of appearance and a vital index to status, power and authority. The police uniform, with its iconic symbolic status, is very important to its wearers in conveying feelings of solidarity and being part of a team. It encourages legitimacy and the group-imposed conformity of its members to be enhanced (Joseph & Alex, 1972). After all, the public expect police officers to at least 'look the part' (Craik, 2005, p. 120) and this has led the stylings of both the mens' and womens' uniforms to be very similar in design.

Despite the ever-growing presence of women in the police over the last 100 years, the traditional masculine work ethos persists, and women still face barriers to inclusion (Silvestri, 2017). The design of the women's police uniform is fundamental

> **There are many industries that still unwittingly embed gendered discrimination through their clothes and the design of their equipment in the workplace. A prime example of this can be found in police uniforms.**

to their integration, acceptance, health, and safety in policing. Previous research has shown that police culture allows a kind of mutual ownership of the police body, and discussions regarding women's 'appearance, body size, and the ability to fit into existing uniforms' are vital (Westmarland, 2017, p. 312). Although workplaces may use gender-neutral language, profess equality and establish unisex dress codes, the work itself is deeply rooted in beliefs about who is expected and accepted to do these roles and the police are no different.

UNISEX = EQUALITY... RIGHT?

The first police uniforms were the very embodiment of the 'ideal male character' (Gorer, 1955, p. 310) and were designed to be masculine since they typically tried to highlight big, strong, male shoulders (Fussell, 2003). When women first joined the police, during the first World War, the donning of the man's uniform was part of the acceptance test (Jackson, 2006), although when women stayed post-war, the clothes underwent a redesign.

There has been lots of changes to womens' uniforms in the UK since their inception. Historically consisting of button-down coats, frill-neck shirts, kitten heels and chunky boots, and truncheons carried in force-branded handbags (see Kirkham, 1996 for a more detailed list of descriptions); there have been many restylings over the last century, in line with changing fashions and recruitment drives (Heidensohn, 1992). Most of the designs were controversial and not fit for purpose (have you ever tried to run after someone in a skirt and heels?).

Recognition of these shortcomings led to the introduction of a unisex uniform in the late 20th century, although some forces were significantly slower than others to buy into the idea. On the surface, the concept of a gender-less uniform was innovative and promised inclusivity, but in reality still only catered for a singular body type. Most gender-neutral items of police clothing are things that can be either sized up or sized down but essentially much of the clothing lacks compatibility with the female body. The original concept of unisex clothing was created in 1968 by Rudi Gernreich, who created a series of garments, including tops and trousers, that women and men could wear interchangeably, but research suggests that clothing of this nature was suitable only for men, and women who had figures similar to men (Morgan, 2019), much like the current police uniform.

These gendered assumptions became apparent shortly after 'unisex' police uniforms were introduced; an officer reported being asked for her collar size upon joining in 2008 (Company Clothing, 2008), and a dog-handler only got her first women's shirt in 2006, after more than 15 years in the force (Haynes, 2007, p. 4).

"It reminds you every day you get dressed that you are in a man's job."

- PC Chapman cited in Haynes, 2007, p. 4

WEARING THE (MEN'S) TROUSERS

Many officers who I spoke to for my research posited that the uniform had significant practical problems and caused worrying health issues. Other UK police research (Stevenson & Black, 2014) surveyed hundreds of officers who lodged complaints regarding most items of their uniforms, but primarily the trousers, stab vests, shirt, polo shirts and boots. My research showed that the current design of the uniform resulted in shirt and jacket sleeves that were far too long, tops that were too short at the back and/or too tight (and revealing) across the chest, painful kit-belts, ill-fitting stab vests, and depending on the force, trousers that were too long or short in the crotch, with outcomes varying from *Candidiasis* (a.k.a. thrush), underwear being revealed and irritation of c-section scars. The rigidity of the trousers can cause discomfort if bloated and tightness can cause period anxiety and/or leakages.

> **...the uniform had significant practical problems and caused worrying health issues.**

In the last few years, one female Inspector campaigned her male bosses about standard-issue trousers until she was finally provided with some money to 'sort it'. Triumphant, she worked with the stores department and sourced various designs to trial. The trousers which worked out best were made by an external company to the police standard, who provided some stretchy trousers that aligned with the current style of her force.

This success at a local level belies a failure country-wide. Back in 2010 a 20-page guide for police forces and uniform manufacturers was written by the British Association of Women's Policing (BAWP). Claire Ames, then-inspector of Devon and Cornwall Police and BAWP member, said she had personally worn trousers for ten years which were neither comfortable nor practical. She commented on the 'unisex' nature of the garments and argued that this does not mean that they are gender-less, more than they are actually 'primarily designed for a male'. Despite seeking to raise awareness of the need for clothing specifically shaped and sized for women, minimal changes have taken place since the guide was published.

One of the problems with thinking about redesigning the uniform is that there has never been one standardised uniform for officers in England and Wales and each of the 43 forces have their own design and procurement teams. Decisions on uniforms are usually made by senior (often male) chief constables or similar, with varying budgets. There are stylistic and practical differences – for example, the kit-belts are one of the pieces of equipment that reportedly sit uncomfortably on women's hips, particularly when the trousers are cut too low, or too high. The weight of the equipment either pulls the belt down or the belt rubs on the hips and waist, sometimes causing bruising. Some forces have eliminated kit belts altogether in favour of tack vests (florescent webbing that cover the stab vest which you can 'hook' your equipment onto), although again, the weight distribution of these are seeing record numbers of women (and even some men) flocking to occupational health with chronic back problems.

© *Brian Jackson* | stock.adobe.com

LIFE-THREATENING PPE

A 2017 Trades Union Congress (TUC) report cited one policewoman who admitted she no longer wears her stab vest at all following her mastectomy because of the discomfort it causes (Prospect, 2016). This, in rare cases, can prove lethal. In 1997, British police officer Nina MacKay was fatally stabbed by a man with schizophrenia after removing her stab vest because it restricted her movement (BBC, 1998). This challenge is not restricted to the UK – in 2016, a Spanish policewoman faced disciplinary action for buying her own stab vest (at a personal cost of £430) because the one issued to her was men's, oversized, and did not offer the appropriate close-fitting protection that she needed.

These problems have been documented on a large scale (Stevenson & Black, 2014), but dismissed due to tight budgets. The stab vests for example are made with mostly flat hard plates, and they do not fit around breasts properly reducing the protection offered. If you have large breasts, the vest rides up exposing the midriff. It also makes it hard for policewomen to reach their guns, handcuffs, and batons. While my research highlights the challenges women face with badly-designed PPE, it seems the design of the stab vest needs changing for everyone – a study in 2009 found that 91% of male and female police officers found their overall stab vest comfort to be either 'neutral or negative' (Barker & Black, 2009).

WHAT'S NEXT?

There are now more than 50,000 women in the police in England and Wales (34.9% of the total). Of new recruits since 2019, 42.5% are women (Gov, 2022). That is a positive development speaking to the increasing diversity of UK policing, but the next part of that story must be about the treatment of those women. The changes that women go through cannot be ignored; pregnancy, childbirth, post-partum issues, maturation, menopause, weight loss/gain, operations (mastectomy, cosmetic enhancements), monthly cycles (this list is not exhaustive). The ill-fitting designs can cause health issues, reduce officer's safety, exacerbate body dysmorphia and lead to low self-esteem. The unisex design is not currently working (men have highlighted problems too). It is vital that all police forces design alternative options and allow staff to make choices about their own bodies, appearance, and personal characteristics. After all, equality isn't about *reducing* the options available – striving for equity means adding *more* options to the wardrobe.

Dr Camilla De Camargo is a lecturer in criminology at Lancaster University Law School. She has published widely in international journals on the topics of 'dirty work', occupational prestige, police well-being and the use of spit hoods. Her main research interest is the police uniform which her PhD was based on (2017). She recently started a blog about sexist dress codes, and tweets sporadically about problems with sexist policies and occupational uniforms in various industries.

Twitter: @DecamargoC

READ MORE

Read more about some of the research that our contributors mention in their articles. We've flagged up those that are open access and given links to online versions where they are available. For full references and citations please visit the online version at *crestresearch.ac.uk/magazine/innovation*

BAELE: AI AND EXTREMISM: THE THREAT OF LANGUAGE MODELS FOR PROPAGANDA PURPOSES

Abid A., et al. (2021). Large Language Models Associate Muslims With Violence. *Nature Machine Intelligence* 3: 461-463. *DOI:10.1038/s42256-021-00359-2*

Bommasani R., *et al*. (2021). On the Opportunities and Risks of Foundation Models. Palo Alto: Stanford Institute for Human-Centered Artificial Intelligence. *arXiv:2108.07258*

Dale R. (2021). GPT-3: What's It Good For? *Natural Language Engineering* 27: 113-118. *DOI:10.1017/S1351324920000601*

Floridi L., Chiriatti M. (2020). GPT-3: Its Nature, Scope, Limits, and Consequence. Minds & Machines 30: 681-694. *https://tinyurl.com/2p9ahm82*

Heaven W. (2020). OpenAI's New Language Generator GPT-3 Is Shockingly Good – And Completely Mindless. MIT Technology Review, 20 July 2020. *https://tinyurl.com/yw2np2zs*

Mor Kapronczay M. (2021). A Beginner's Guide to Language Models. Towards Data Science, 8 January 202, *https://tinyurl.com/cmrw7eus*

Urbina F., Lentzos F., Invernizzi C., Ekins S. (2022). Dual Use of Artificial-Intelligence-Powered Drug Discovery. *Nature Machine Intelligence* 4: 189-191. *DOI:10.1038/s42256-022-00465-9*

Weidinger L., et al. (2021). Ethical and Social Risks of Harm from Language Models. *arXiv:2112.04359*

BRACE: THE 'INCELOSPHERE' AND INCEL VIOLENCE: A WORSENING PROBLEM?

Baele, S., Brace, L. and Ging, D. (2023). A Diachronic Cross-Platforms Analysis of Violent Extremist Language in the Incel Online Ecosystem, *Terrorism and Political Violence,* pp. 1–24. *DOI:10.1080/09546553.2022.2161373*

Baele, S.J. et al. (2022). Super- (and hyper-) posters on extremist forums, *Journal of Policing, Intelligence and Counter Terrorism*, pp. 1–39. *DOI:10.1080/18335330.2022.2103386*

Brace, L. (2021). *A Short Introduction To The Involuntary Celibate Sub-Culture. https://tinyurl.com/bydhnuua*

Broyd, J. et al. (2022). Incels, violence and mental disorder: a narrative review with recommendations for best practice in risk assessment and clinical intervention, *BJPsych Advances*, pp. 1–11. *DOI:10.1192/bja.2022.15*

Hutchinson, J. et al. (2022). Violent Extremist & REMVE *Online Ecosystems: Ecological Characteristics for Future Research & Conceptualization*. RESOLVE Network. *DOI:10.37805/remve2022.5*

Moskalenko, S. et al. (2022). Predictors of Radical Intentions among Incels: A Survey of 54 Self-identified Incels, *Journal of Online Trust and Safety*, 1(3). *DOI:10.54501/jots.v1i3.57*

O'Malley, R.L., Holt, K. and Holt, T.J. (2020). An Exploration of the Involuntary Celibate (Incel) Subculture Online, *Journal of Interpersonal Violence*, p. 088626052095962. *DOI:10.1177/0886260520959625*

Scrivens, R. et al. (2021). Examining Online Indicators of Extremism in Violent Right-Wing Extremist Forums, *Studies in Conflict & Terrorism*, pp. 1–25. *DOI:10.1080/1057610X.2021.1913818*

BUCKLEY: ROLLING THE DICE ON ALGORITHMS: INCREASING UNDERSTANDING THROUGH BOARDGAMES

Jones, W. and Teytelboym, A., (2017). The international refugee match: A system that respects refugees' preferences and the priorities of states. *Refugee Survey Quarterly*, 36(2), pp.84-109. *DOI:10.1093/rsq/hdx004*

Jones, W. and Teytelboym, A., (2018). The local refugee match: Aligning refugees' preferences with the capacities and priorities of localities. *Journal of Refugee Studies*, 31(2), pp.152-178. *DOI:10.1093/jrs/fex022*

Noda, S., Shirotsuki, K. and Nakao, M., (2019). The effectiveness of intervention with board games: a systematic review. *BioPsychoSocial medicine*, 13(1), pp.1-21. *DOI:10.1186/s13030-019-0164-1*

ChatGPT: AI INNOVATION RISKS & IMPLICATIONS

These references were generated by ChatGPT:

Calo, S., A. (2015). Artificial Intelligence and the Future of Privacy, *Washington Law Review*, vol. 90, no. 3, pp. 1023–1077.

Corker, D., L. and Walker, A. (2016). The ethics of artificial intelligence, *Nature*, vol. 536, pp. 457-460.

O'Neil, K. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, Crown.

Parsai, G. (2018). AI systems and job displacement: exploring the challenges and opportunities, *International Journal of Information Management*, vol. 42, pp. 18-26.

Spengler, J., C. (2021). Cybersecurity and artificial intelligence, *Communications of the ACM*, vol.

DOCTOR, ELSON & HUNTER: VIOLENT EXTREMISM, INNOVATION, AND RECRUITMENT IN THE METAVERSE

Binder, J. F., & Kenyon, J. (2022). Terrorism and the internet: How dangerous is online radicalization? *Frontiers in psychology*, 6639. *https://tinyurl.com/j7bfxpaz*

Cragin, R. K. (2022). Virtual and Physical Realities: Violent Extremists' Recruitment of Individuals Associated with the US Military. *Studies in Conflict & Terrorism*, 1-22. *DOI:10.1080/1057610X.2022.2133346*

Elson, J. S., Doctor, A. C., & Hunter, S. (2022). The metaverse offers a future full of potential–for terrorists and extremists, too. The Conversation. *https://tinyurl.com/2ycxm65u*

Hunter, S. T., Shortland, N. D., Crayne, M. P., & Ligon, G. S. (2017). Recruitment and selection in violent extremist organizations: Exploring what industrial and organizational psychology might contribute. *American Psychologist,* 72(3), 242. *DOI:10.1037/amp0000089*

Lee, L. H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., & Hui, P. (2021). All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda. *arXiv:2110.05352*

Ortiz, L. (2022). Risks of the Metaverse: A VRChat Study Case. *The Journal of Intelligence, Conflict, and Warfare*, 5(2), 53-128. *DOI:10.21810/jicw.v5i2.5041*

DE CAMARGO: WHEN THE UNIFORM DOESN'T FIT

Barker, J. & Black, C. (2009). Ballistic vests for police officers: using clothing comfort theory to analyse personal protective clothing, *International journal of fashion design, technology and education*, 2(2-3), pp. 59–69. *DOI:10.1080/17543260903300307*

BBC. (1998). Man admits manslaughter of WPC, 22nd October, *BBC News Online*, *www.news.bbc.co.uk/1/hi/uk/79569.stm*

Cave, A. (2016). Do different uniforms for boys and girls amount to sex discrimination? *https://tinyurl.com/3edtu25f*

De Camargo, C. R. (2017). *A Uniform Not Uniform*, Unpublished PhD Thesis, University of Salford.

Fussell, P. (2003). *Uniforms: Why We Are What We Wear*. New York: Houghton Mifflin. *https://tinyurl.com/4nbunamr*

Goldstein, A. N. (2018). CNO, Are you listening? Why uniforms matter to female officers. Proceedings, Vol. 144/8/1,386. *https://tinyurl.com/4wmv3x9e*

Joseph, N., & Alex, N. (1972). The Uniform: A Sociological Perspective. *American Journal of Sociology*, 77, 719-730. *DOI:10.1086/225197*

HENDERSON: THE DISINFORMATION GAME: FINDING NEW WAYS TO FIGHT 'FAKE NEWS'

Hakala J., & Melnychuk J., (2021). Russia's Strategy in Cyberspace. Riga: NATO Strategic Communications Centre of Excellence, *https://tinyurl.com/y8rfwfae*

Kaminska, I. (2017). A lesson in fake news from the info-wars of ancient Rome. Financial Times. *https://tinyurl.com/ywa96xz3*

Lloydlangston, A., & Lo, T. (2008). The POW Will Safely Return!: Second World War Allied and German Propoganda. Canadian Military History, 17(3), 6. *https://tinyurl.com/yzfswwxp*

Parsons, C., Drünkler, A., Born, D., Fuest, K., Gschwendtner, C., & Krys, C. (2019). Democracy and digital disinformation *https://tinyurl.com/yc37pebh*

Roozenbeek, J., & van der Linden, S. (2019). The fake news game: actively inoculating against the risk of misinformation. *Journal of Risk Research*, 22(5), 570–580. *DOI:10.1080/13669877.2018.1443491*

HOPE, KONTOGIANNI & DE LA FUENTE VILAR: HOW DID YOU ESCAPE? A RAPPORT-BASED FRAMEWORK FOR TIME-CRITICAL QUESTIONING INVOLVING COOPERATIVE INTERVIEWEES

Hope, L. (2016). Evaluating the Effects of Stress and Fatigue on Police Officer Response and Recall: A Challenge for Research, Training, Practice and Policy. *Journal of Applied Research in Memory and Cognition*. 5. 239-245. *DOI:10.1016/j.jarmac.2016.07.008*

Hope, L., Kontogianni, F., Thomas, W., & De la Fuente Vilar, A. (forthcoming). Eliciting information in time-critical contexts: Development and testing of the Time-Critical Questioning Framework

LEE, REDER & GREIG: EXTREME RIGHT-WING TERRORISM IN THE UK

Ashby, H. (2021). Far-Right Extremism Is a Global Problem, *https://tinyurl.com/4exebtjz*

Conway, M., and Dillon, J., (n.d.) Case Study: Future trends live-streaming terrorist attacks? *https://tinyurl.com/mryeg9wew*

MASON: IS 'GOVERNMENT' AND 'INNOVATION' AN OXYMORON? PUBLIC SECTOR INNOVATION: A PRACTITIONER'S PERSPECTIVE

Douglas, K.M., Druckman, J.N., & Drury, J. (2020). Using social and behavioural science to support COVID-19 pandemic response. *Nature human behaviour*, 4(5), pp.460-471. *DOI: 10.1038/s41562-020-0884-z*

Galvao, A., Mascarenhas, C., Marques, C., Ferreira, J., & Ratten, V., (2019). Triple helix and its evolution: a systematic literature review, *Journal of Science and Technology Policy Management*. *DOI:10.1108/JSTPM-10-2018-0103*

Mason, L., & Shortland, A. (2022) National Security Innovation: Creating new capabilities for the future, *CETaS Expert Analysis, https://tinyurl.com/bdzjy4c5*

Reeder, N. (2020). Organizational culture and career development in the British civil service, *Public Money & Management*, 40:8, 559 568, *DOI: 10.1080/09540962.2020.1754576*

S, A., Killworth, P. (2022) Reinventing National Security: Innovation, Diversity and Inclusion, *CETaS Expert Analysis*, *https://tinyurl.com/4dm22db2*

PHELAN, WHITE, PATERSON & WALLNER: MISOGYNY AND MASCULINITY: TOWARD A TYPOLOGY OF GENDERED NARRATIVES AMONGST THE FAR-RIGHT

The Southern Poverty Law Centre's overview of 'Male Supremacy', *https://tinyurl.com/2r7nw2kb*

RICE & INNES: WHAT'S NEW, WHAT WORKS? COUNTERING-TERRORISM WITH PUBLIC-FACING STRATEGIC COMMUNICATION CAMPAIGNS

Heath, R.L., Lee, J., Palenchar, M.J., & Lemon, L.L. (2017). Risk Communication Emergency Response Preparedness: Contextual Assessment of the Protective Action Decision Model. *Risk Analysis*, 38(2): 333-344. *DOI:10.1111/risa.12845*

Rice, C., Stanton, E.E., & Taylor, M. (2021). A Communication Toolkit to Build Trust: Lessons from Northern Ireland's Civil Society Peacebuilders. *VOLUNTAS*, 32: 1154–1164. *DOI:10.1007/s11266-021-00376-0*

SHAW, SIBBONS, CONCHIE & TAYLOR: ARE EMERGING DIGITAL BEHAVIOURAL BIOMETRICS ABLE TO IDENTIFY US?

Information Commissioner's Office. (2022a). *Biometrics: Foresight, https://tinyurl.com/bdzf5wsr*

Information Commissioner's Office. (2022b). *Biometrics: Insight*, *https://tinyurl.com/yc7uz2xk*

STEEN: A COMMUNICATION PERSPECTIVE ON RESILIENCE

Afifi, T.D., Merrill, A.,& Davis, S. (2016). The theory of resilience and relational load. *Personal Relationships*, 23, 663-683. *DOI:10.1111/pere.12159*

Buzzanell, P. M. (2018). Communication theory of resilience. In D.O. Braithwaite, E. A. Suter, & K. Floyd (Eds.), Engaging theories in family communication: Multiple perspectives (2nd ed., pp. 98-109). Routledge. *DOI: 10.4324/9781315204321-9*

Chairman of the Joint Chiefs of Staff Instruction (2011, Sept 1). Chairman's total force fitness framework (CJCSI 3405.01). Office of the Chairman of the Joint Chiefs of Staff. *https://tinyurl.com/2ntm5e8v*

Goodwin, G. F., Blacksmith, N., & Coats, M. R. (2018). The science of teams in the military: Contributions from over 60 years of research. American Psychologist, 73(4), 322-333. *DOI:10.1037/amp0000259*

Pearce, W. B. (1989). *Communication and the human condition*. Illinois University Press.

Pearce, W. B., & Cronen, V. E. (1980). *Communication, action, and meaning: The creation of social realities.* Praeger. *https://tinyurl.com/4bha3xth*

Penman, R. (2014). Coordinated Management of Meaning (CMM). *Key Concepts in Intercultural Dialogue*. *https://tinyurl.com/yckkh97s*

Whitt, J. E, & Steen, S. L. (2021). Talking and listening to build a stronger military: Cosmopolitan communication as an essential skill of military leader development. *Journal of Character & Leadership Development,* 8(1), 190-204. *https://tinyurl.com/46c43tz9*

CENTRE FOR RESEARCH AND EVIDENCE ON SECURITY THREATS

CREST Security Review provides a gateway to the very best knowledge and expertise. Its articles translate academic jargon to 'so what' answers and illustrate how behavioural and social science can be used effectively in everyday scenarios.

THE CENTRE FOR RESEARCH AND EVIDENCE ON SECURITY THREATS

CSR is produced by the Centre for Research and Evidence on Security Threats (CREST). CREST is funded by the UK's Home Office and security and intelligence agencies to identify and produce social science that enhances their understanding of security threats and capacity to counter them. CREST also receives funding from its core partners (the universities of Bath, Lancaster and Portsmouth). Its funding is administered by the Economic and Social Research Council (ESRC Award ES/V002775/1), one of seven UK Research Councils, which direct taxpayers' money towards academic research and training. The ESRC ensures the academic independence and rigour of CREST's work.

CREST has established a growing international network of over 140 researchers, commissioned research in priority areas, and begun to tackle some of the field's most pressing questions.

> '*CREST Security Review is a fantastic means by which we can keep practitioners, policy-makers and other stakeholders up-to-date on the impressive social and behavioural science occurring not only at CREST, but around the world.*'
>
> Professor Stacey Conchie, CREST Director

For more information on CREST and its work visit **www.crestresearch.ac.uk** or find us on Twitter, @crest_research