WINTER 2024 / ISSUE 18

CREST SECURITY REVIEW

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

Communication

CONTENTS

CREST SECURITY REVIEW
Editor – Rebecca Stevens
Co-Editors – Anna Leslie & Kayleigh Brennan
Illustrator – Rebecca Stevens
Designer – Kayleigh Brennan
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

Communication; the transmission of information. This crucial aspect of human interaction bridges understanding, empowers action, and shapes responses to imminent dangers.

In this issue of *CREST Security Review* (*CSR*), we unravel the behavioural and social science behind communication's role in deciphering, managing, and countering threats.

We start by exploring the complex process of sensemaking and disclosure in investigative interviews. David A. Neequaye introduces a sensemaking approach that sheds light on individual motivations for divulging information (p. 4), followed by Mattias Sjoberg's latest research on Taylor's Cylinder Model for understanding sensemaking, especially in suspect interactions (p. 6). Lastly, Nick van der Klok *et al.* (p. 8) investigate negotiators' potential to accelerate their influence over a suicidal person in crisis.

Continuing, we delve into the vital components of trust and rapport in communication; Lina Hillner (p. 10) examines the impact of perceived interviewer trustworthiness, while Lorraine Hope navigates strategies for overcoming cross-cultural challenges in rapport building (p. 12).

Shifting our focus to misconceptions, Vincent Denault and Aldert Vrij challenge traditional beliefs about nonverbal communication, offering insights into its role in discerning truth from deception (p. 14).

Moving forward, we explore the significance of information sharing in security. Dana Roemling and Jack Grieve (p. 18) shed light on the underestimated tool of forensic authorship analysis, while Becky Phythian discusses enhancing law enforcement through improved information-sharing practices (p. 20).

Finally, we explore how technology shapes communication dynamics. Laura G. E. Smith (p. 22) investigates digital traces of offline mobilisation, Laura Stevens examines digital technologies in documenting gender-based violence (p. 24), Anastasia Kordoni explores language's role in expressing social identities and influencing online communities (p. 26), and Marc Kydd *et al.* discuss enhancing romance fraud prevention (p. 28).

Additionally, we feature articles addressing broader aspects of security research: Nadine Salman and Zainab Al-Attar examine the contextual relevance of neurodivergence within extremist populations (p. 30), Austin Doctor *et al.* investigate how militant leaders' exposure to violence predicts their tactics and strategies (p. 32), Rachel Monaghan and Bianca Slocombe analyse the prosecution landscape for extremist actors in the UK (p. 34), and Joel Busher *et al.* delve into radicalisation and counter-radicalisation research (p. 36).

For further exploration, refer to the 'Read More' section for research underpinning our articles and additional reading. We value your feedback on this issue and welcome your suggestions for future topics. Please share your thoughts via the provided survey link or QR code. Thank you.

Rebecca 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.

DAVID A. NEEQUAYE

HOW PEOPLE DECIDE WHAT TO DISCLOSE IN INVESTIGATIVE INTERVIEWS

This article offers a sensemaking approach to investigative interviewing that better anticipates what people may decide to divulge in interviews.

> *"[...] [T]he brother should be careful not to give the enemy any vital information* (p. 159). *[...]. During the interrogation, say only the things that you agreed upon with your commander. Do not be concerned about other brothers* (p. 168)."
>
> (The Al-Qaeda Training Manual)

The above excerpt is part of the guidance given to Al-Qaeda operatives who find themselves in an investigative interview. Such interviews are social interactions in which law enforcement interviewers seek information from people (i.e., interviewees) for security or legal reasons. My collaborators and I have begun to examine how interviewees, for example, Al-Qaeda operatives, decide what to disclose. Existing research heavily focuses on the amount of information interviewees reveal, which assists in grasping what makes interviewees communicate. However, we need to know precisely what interviewees disclose and why they choose to share the information they do. What counts as vital information from an Al-Qaeda commander and operative point-of-view?

We offer a sensemaking approach to investigative interviewing that better anticipates what interviewees might decide to say. Accounts indicate that interviewees typically face *conflicting motivations* to co-operate with the interviewer when being questioned.

A. They perceive that disclosing some information might help them achieve material benefits—for example, a lesser prison sentence. That possibility could keep an Al-Qaeda operative engaged in speaking about things previously sanctioned by their commander. So on certain topics, they may be willing to co-operate.

B. They safeguard certain self-interests, leading to the withholding of some information. For example, the instruction by the Al-Qaeda manual not to reveal vital information, lest the revelation disrupt a planned attack. On these subjects, interviewees will be less likely co-operate.

My collaborators and I predicted that sanctioning what an operative can reveal and the so-called vital information (to conceal) arises from a cost-benefit analysis. That process determines what could be disclosed to reveal benefits and avoid costs safely. This sensemaking leads us to hypothesise that interviewees might view any given piece of information an interviewer requests across two axis: low to high stakes, and whether it should be guarded or unguarded.

> **We predict that interviewees need little to no convincing to disclose low-stakes or unguarded information.**

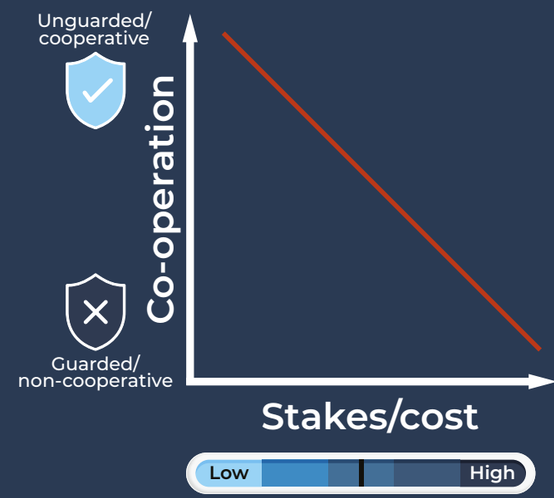
1. Low Stakes information is unguarded

Some information could be viewed as unlikely to attract a cost. That is to say, its disclosure is unlikely to assist in thwarting a planned Al-Qaeda attack, for example. Simultaneously, revealing such information might make the interviewee appear cooperative or willing to engage. These are the things an Al-Qaeda commander is likely to sanction an operative to disclose. We predict that interviewees need little to no convincing to disclose low-stakes or unguarded information.

2. High Stakes information is guarded

Conversely, some information could be viewed as costly to reveal—things that might foil an imminent terror plot, returning little tangible benefits to Al-Qaeda, for example. These are the things that the Al-Qaeda manual views as vital and warns operatives to refrain from disclosing when being interviewed.

MOVING TO DISCLOSURE: THE JOURNEY FROM GUARDED TO UNGUARDED



We predict that if an interviewer gets an interviewee to disclose such information, it means the interviewer somehow managed to influence the interviewee's cost-benefit calculations—such that what was high-stakes now resembles low-stakes information.

It is worth noting that what becomes low-stakes, unguarded, high-takes, or guarded information is complex. Things can change depending on the interviewee and the specific circumstances that led to the interview. For example, commanders and operatives might categorise different things as vital information depending on specific Al-Qaeda missions and cells. *"During the interrogation, say only the things that you agreed upon with your commander. Do not be concerned about other brothers (The Al-Qaeda Training Manual p. 168)."* Being cognisant that, generally, interviewees determine what to disclose via (an intuitive) cost-benefit analysis can simplify the understanding of the mechanisms underlying disclosure—while allowing practising interviewers to appreciate the complexity specific scenarios bring.

RISK APPETITE

Our recent research, which frames scenarios such that some information is riskier to disclose than others, supports the cost-benefit sensemaking approach to disclosure in interviews. Interviewees typically share information they perceive would achieve benefits while taking minimal risks. People are most forthcoming with details whose features resemble unguarded information and most unyielding with things they perceive would be costly to disclose (i.e., guarded information). However, when examining low- versus high-stakes information, we have also found that there was a high level of individual variance in assessing what was risky to disclose. Sometimes, interviewees prefer taking the risk of disclosing high-stakes information; other times, they play it safe and stick to disclosing low- rather than high-stakes information. Risk appetite depends heavily on the **specific circumstances surrounding a specific interview**. Thus, it is crucial for interviewers to continually strive to decipher the topics an interviewee deems more or less risky to converse about. Then, interviewers can adapt accordingly to elicit the particular information they seek. We hope to build on this budding sensemaking approach to assist researchers in developing practically relevant studies and help practitioners better anticipate how interviewees might behave.

David A. Neequaye is a lecturer in Social Psychology at Lancaster University. His research primarily examines how individuals ask and answer questions, emphasising conversations related to security concerns.

MATTIAS SJÖBERG

INTERPERSONAL SENSEMAKING: A POWERFUL TOOL FOR FACILITATING COOPERATION IN SUSPECTS

By making sense of a suspect's goals and motivations, an investigative interviewer may facilitate a positive process of interpersonal sensemaking that eventually can build trust and cooperation.

Imagine being a freshly minted investigative interviewer about to enter an interview with a suspect. As you enter the interview, you wonder how best to frame the interaction. Should you limit the discussion to the facts only? Perhaps it might be better to explore the suspect's feelings and worries about their future? What about trying to be friends and crack some jokes to make them feel better? The answer to these questions is not simple. Recent research on interpersonal sensemaking in investigative interviews can offer some insights.

Used by investigative interviewing and crisis negotiation teams around the world, interpersonal sensemaking is a framework for understanding the way people communicate and the goals and motivations that underlie those ways. At any one point in time, suspects tend to focus their goals and motivations around instrumental (facts and information), relational (establishing or breaking down the relationship with their interviewer), or identity (personal needs and wants) issues.

> **...suspects tend to focus their goals and motivations around instrumental (facts and information), relational (establishing or breaking down the relationship with their interrogator), or identity (personal needs and wants) issues.**

In my PhD research together with my supervisors at Lancaster University, we have been investigating (i) how to successfully develop interpersonal sensemaking in investigative interviews through matching (i.e., coordination) of these motivations, and (ii) what consequences it has on interview outcomes and reciprocal matching. This is what we have found.

MATCHING OF MOTIVATION IS KEY

Across several experiments, involving hundreds of participants, we have found that focusing on similar issues, (i.e., motivational matching) consistently led to more positive investigative interview outcomes. In other words, suspects who interacted with an interviewer who consistently made sense of their goals and motivations were more willing to cooperate and felt more understood compared to those whose interviewer did not make sense of them (i.e., did not match their motivations). Interviewees were often more willing to trust the interviewer. Hence, successful interpersonal sensemaking might be a shortcut to building trust and positive working relationships.

Interestingly, suspects who interacted with an interviewer who made sense of their goals through motivational matching also displayed more reciprocal motivational matching. That is, they increasingly started to match the interviewer's goals and motivations back. This constitutes a form of entrainment, where the interviewer's adjustment on the motivational frames leads to similar, synchronised changes in the suspect's motivations.

As an investigative interviewer, making sense of a suspect's goals and motivations is likely important. For example, asking for meticulous details about the suspect's whereabouts while they voice concern about the wellbeing of their friends and family might not be the best strategy. Why? The question is focused on an instrumental goal while the suspect's needs are rooted in their worries about their friends and family (identity motivations). Getting into the same frame as the suspect is the first step in starting to understand their wants and needs and how to best address them. Hence, being able to identify a suspect's goals and motivations and then matching those, ought to be an important skill for any investigative interviewer worthy of their craft.

IS MATCHING ALWAYS POSITIVE?

It is easy to assume that motivational matching works under any circumstance. However, there are situations when matching can backfire. For example, in our experiments, we have found that when the investigative interviewer and suspect were arguing with each other (they were both in a competitive orientation), motivational matching generally led to worse interview outcomes. More interestingly, this was particularly true when they were attacking each other's identity or the relationship they had with each other (i.e., identity and relational matching), rather than focusing exclusively on the problem (i.e., instrumental matching).

This has potential implications for investigative interviewers. In essence, if you absolutely must argue with someone, it is probably wise to strive to keep the conversation on topic. At all costs, avoid reciprocating negative behaviours such as ridicule or personal insults, as these might force the interview down a negative spiral of conflict and stalemate.

In a complex social interaction such as an investigative interview, failure to accurately plan and prepare could be costly. Interpersonal sensemaking in general, and motivational frame matching in particular, may offer a simple framework for starting to help make sense of conversations with suspects. This, in turn, may constitute the first building blocks to establishing a relationship with them that can eventually promote cooperation and trust.

> **...the investigative interviewer and suspect were arguing with each other (they were both in a competitive orientation), motivational matching generally led to worse interview outcomes.**

Mattias Sjöberg is a postdoctoral research associate at Durham University Business School. He researches how people make sense of each other in interpersonal, intergroup, and leadership situations. His Twitter (X) handle is: @DrMattiasSjoberg.

NICK VAN DER KLOK, MIRIAM OOSTINGA, LUKE RUSSELL & MICHAEL YANSICK

ACCELERATING INFLUENCE: CHALLENGING THE LINEAR PARADIGM OF SUICIDE NEGOTIATION

This article provides new insights from crisis negotiation practitioners and researchers. Specifically, on whether a negotiator can accelerate their influence over a suicidal person in crisis.

TRADITIONAL CRISIS NEGOTIATION MODELS

Suicide negotiation is a high-stakes, complex and unpredictable task that specialised police officers (i.e., negotiators) perform on a day-to-day basis. The goal of the negotiator is to save the life of the person in crisis. The question is, however, how to reach that goal without someone getting hurt? To bring order to these unstable interactions, law enforcement agencies and academics have collaborated, researched and constructed simplified negotiation models for hostage, terrorist and suicide negotiations. The latter model being called: the revised Behavioural Influence Stairway Model (see figure 1); specifically tailored for dealing with mentally unstable individuals considering or attempting suicide.

> **The stairway model provides the negotiator with a path towards behavioural change of the person in crisis.**

In essence, the stairway model provides the negotiator with a path towards behavioural change of the person in crisis, and consists of four sequential stages:

1. **EMPATHY** – trying to understand the situation, feeling and motives of the subject.
2. **RAPPORT** – creating a smooth, positive and harmonious connection with the subject.
3. **TRUST** – being perceived as honest, sincere and capable of delivering on promises.
4. **INFLUENCE** – inducing a change in the subject's state of mind.

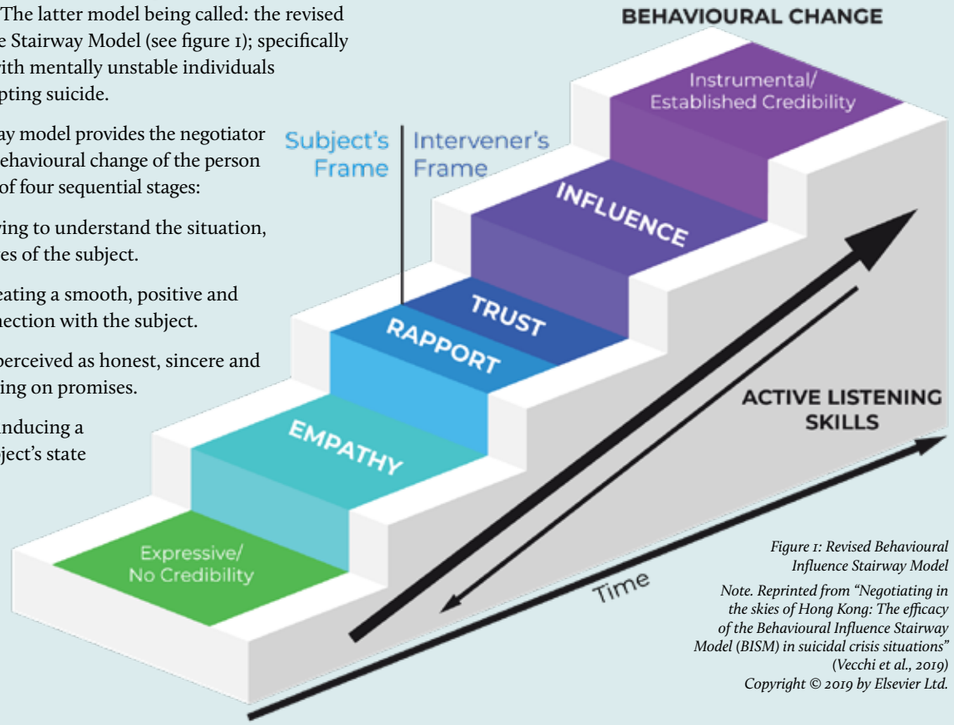


Figure 1: Revised Behavioural Influence Stairway Model

Note. Reprinted from "Negotiating in the skies of Hong Kong: The efficacy of the Behavioural Influence Stairway Model (BISM) in suicidal crisis situations" (Vecchi et al., 2019)

The underlying mechanism of this stairway metaphor is based on the axiom of linearity. Meaning, one stage (e.g., empathy) must first be completed before the other stage (e.g., rapport) can occur. Following this line of reasoning, behavioural change is only possible if all stages (empathy, rapport, trust and influence) are sequentially achieved. Vecchi et al. explicitly state: "Behavioral change will occur only if the previous four stages have been successfully completed".

REAL-LIFE EXPERIENCES OF PRACTITIONERS

Although practitioners generally view the stairway model as a good foothold during negotiations, there have been cases where negotiators deviate from the theory. The third and fourth contributors to this article experienced opportunities for *accelerated influence* in their decades of crisis negotiation practices, including hostage, terrorist and suicide negotiations. They confirmed the mutual occurrence of this phenomenon through a survey with 84 negotiators from 14 different countries, of which 78% agreed to have experienced the same in (some of) their operations. Accelerated influence can be described as short-circuiting the negotiation, omitting one or more of the stairway stages (e.g., empathy, rapport, or trust), reaching influence quickly and establishing different types of behavioural change early in the negotiation.

EMPIRICAL EXPERIMENTATION

To explore this phenomenon of accelerated influence, researchers at the University of Twente (Netherlands) began investigating its effect in the suicide negotiation setting. In an online pre-programmed suicide negotiation, two negotiation styles were compared: the traditional approach versus accelerated approach. Through various methods (video, script and an imagination exercise) participants were immersed in a fictitious situation where they were standing at the edge of a bridge contemplating suicide. Subsequently, they were contacted by a negotiator via text-messages. In random order, the negotiator performed either an accelerated approach (directly asking for a behavioural change followed by the stairway stages) or the traditional approach (following the stairway stages and then asking for a behavioural change); without the participants knowing which treatment they received. To illustrate, in the accelerated approach, the crisis negotiator immediately asked for a change in behaviour of the participant: *"I can see you from a distance and I get really frightened when I see you at the other side of the fence, because I think you might fall by accident before you are ready. Why don't you come to the other side of the fence, so we can continue this conversation in a safer manner?"*. Whereas, in the traditional approach, the crisis negotiator first attempted to build a relationship based on empathy, rapport and trust with the participant before asking for a change in behaviour. For example, the negotiator tried to establish trust by saying: *"I am here for you and will do all that I can to support you. It may feel like you were alone in this before we started talking, to reassure you I do have experience supporting people in similar situations in finding a way forward"*. Overall, the experiment confirmed the efficacy of the traditional approach, showing a 55% compliance rate towards the crisis negotiator's safety suggestion (i.e., behavioural change). However, in 32% of the cases, the negotiator was able to reach behavioural change from the onset of the interaction. Even more so, both groups ended with medium to high levels of empathy, rapport, and trust. Thus, even a failed accelerated attempt did not seem to harm the relationship between the crisis negotiator and participant.

> **In 32% of the cases, the negotiator was able to reach behavioural change from the onset of the interaction.**

DISCUSSION AND FUTURE EXPLORATION

While the early evidence, indicating the potential for accelerated influence, is certainly promising, it is essential to validate these findings through additional studies that incorporate face-to-face interactions. Besides, it is worth noting that the sample consisted mainly of participants with a Western background (45% Dutch, 35% German). Therefore, future studies could explore potential differences in achieving accelerated influence between Western and non-Western individuals. Last, the current study focused on suicide negotiations. Future research could investigate whether the effect of accelerated influence is similar in hostage and terrorism negotiations. Nonetheless, the practical and academical discovery of accelerated influence in suicide crisis negotiation can initiate a thought-provoking discussion about re-evaluating the conventional stairway metaphor. One could consider a more nuanced version of the stairway model, or even start envisioning different types of new metaphors. For example, a climbing wall metaphor consisting of:

- Multiple deployment routes which offer various approaches to reach a safe resolution.
- Different paths of varying complexity suitable for negotiators of different experience levels; from 'linear and structured' to 'non-linear and flexible' routes.
- Shortcuts that allow negotiators to skip stages when feasible.

With this article, we hope to encourage scholars and practitioners to join this conversation and rethink the linear proposition, visualise and test different metaphors for improved negotiation training and conduct further empirical research into the phenomenon of accelerated influence.

Nick van der Klok is a master of science graduate in social psychology at the University of Twente. Miriam S. D. Oostinga is Assistant Professor at the Psychology of Conflict, Risk and Safety section of the University of Twente. Luke C. Russell is a Detective Chief Inspector with Leicestershire Police, UK. Michael A. Yansick is a Supervisory Special Agent with the FBI, USA.

LINA HILLNER

UNEXPLORED INTERACTIONS: DISENTANGLING TRUSTWORTHINESS, TRUST AND RAPPORT

How does an interviewer's perceived trustworthiness and rapport-building influence interview outcomes? This article delves into the individual impact of these processes on information disclosure and explores their potential interaction.

Effective communication plays a crucial role in human interactions, with its significance particularly pronounced in law enforcement and security contexts. Lapses in communication, miscommunications, or errors in interactions with officers, source handlers or other security personnel can have profound and lasting repercussions for investigations and the efficacy of intelligence gathering. For this reason, effective interactions between interviewers and interviewees are crucial, irrespective of whether the interviewee is a suspect, witness, victim or source. To enhance statement quality and boost reliability, evidence-based interviewing models advocate a rapport-based approach. More recently, scholars have turned their attention to understanding the role of trust in information gathering contexts.

THE ROLE OF TRUSTWORTHINESS AND TRUST IN INFORMATION GATHERING

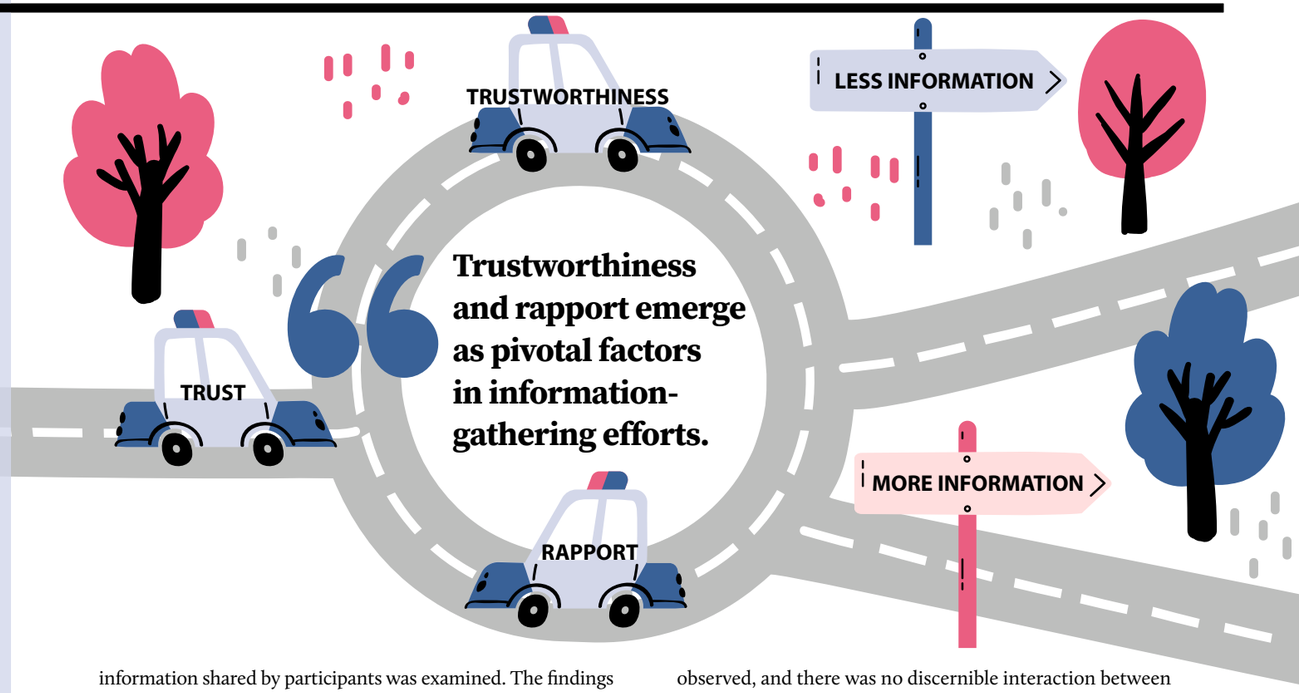
During encounters, we continuously evaluate an individual's trustworthiness based on their competence (capability to perform a task), integrity (commitment to promises), and benevolence (demonstrated goodwill). Our assessment of another person's trustworthiness influences our willingness to trust them and, consequently, shapes our engagement in risk-taking behaviours. In intelligence gathering, instances of risk-taking may involve disclosing sensitive information that jeopardises the safety of the source, or sharing information that could be used to incriminate another individual. Now researchers have begun to explore how trustworthiness and trust impact investigative interviews and intelligence gathering efforts.

Drawing from case studies of real-life investigators, two trust-building strategies have been observed and studied: demonstrating trustworthiness and showing a willingness to trust. Under experimental conditions, trustworthiness (i.e., integrity) was demonstrated through an interviewer making and fulfilling a promise (e.g., promising to retrieve the mock-source's phone), while the willingness to trust involved the interviewer demonstrating vulnerability to the mock-source (e.g., by trusting them with a key to a restroom near high-value equipment). Results suggest that interviewers who demonstrated their trustworthiness increased the mock-source's trust, which enhanced cooperation and led to greater disclosure of relevant information. In contrast, the interviewer's demonstration of vulnerability to the source had no impact on how much trust the source had in the interviewer. It seems likely that the success of this trust-building strategy is conditional upon the pertinence of the offer (e.g., needing to go to the restroom). To advance our understanding of how to quickly build trust, future research should investigate the relative importance of competence, integrity, or benevolence in the trust-building process.

THE EFFECTS OF RAPPORT-BUILDING ON INFORMATION GAIN

In contrast to trust, rapport and its impact on outcomes in information gathering has been extensively studied. Rapport can be defined as the quality of the interaction between the interviewer and the interviewee. The popular tripartite model of rapport posits that this quality can be characterised by the extent to which both parties exhibit attentiveness (mutual attention), maintain a friendly and respectful demeanour (positivity), and smoothly transition between topics (coordination). Interviewers who successfully build and maintain rapport are perceived more positively and tend to elicit higher amounts of accurate information than interviewers who neglect rapport-building efforts. Building rapport with an interviewee appears to increase willingness to cooperate, and, as a result, increases the amount of information shared. It is, therefore, unsurprising that rapport-building seems to mitigate counter-interrogation tactics (CITs), such as passivity or providing a 'no comment' response.

Numerous rapport-building strategies exist, and several have been subject to empirical investigation. In a recent study, the impact of reciprocal self-disclosure on the extent of crime-relevant



information shared by participants was examined. The findings suggest when interviewers and participants sought and discussed commonalities, it created a sense of connection (i.e., rapport), which in turn, improved cooperation and made participants share more relevant information when questioned. Similar to trust-building, rapport-building appears to indirectly boost information disclosure by facilitating interviewees' willingness to cooperate.

THE INTERSECTION OF RAPPORT AND TRUST

While trust and rapport seem to operate in a similar fashion, their interaction might lead to different interview outcomes. Consider this scenario: you encounter an interviewer you initially perceive as untrustworthy. However, during the following interview, they adopt an overly friendly approach in an attempt to build rapport. According to theories on expectancy violations, this rapport-building effort could backfire and heighten your suspicions. The incongruence between the interviewer's friendliness and your initial perception may exacerbate your concerns about their trustworthiness. Conversely, some research suggests that beliefs are adaptable. Adopting this perspective, you might reinterpret their rapport-building as friendly, correcting your initial perception and arriving at a more neutral standpoint.

To test these contrasting predictions, our recent research manipulated the interviewer's trustworthiness (untrustworthy vs trustworthy) and rapport-building attempts (present vs absent) and investigated the impact on disclosure of sensitive information in a simulated job interview conducted through a chat interface. Findings revealed a decrease in the participants' trust in the interviewer when they perceived them as untrustworthy, consequently reducing the amount of sensitive information disclosed during the interview. Interestingly, no significant effects of rapport on interview disclosure were observed, and there was no discernible interaction between rapport-building and perceived trustworthiness. That means, contrary to predictions, interviewers who build rapport did not elicit more information from participants than interviewers who refrained from rapport-building. Given the professional context of a job interview, participants' might not have expected the interviewer to be overly friendly, and, in turn, might not have judged the lack of rapport harshly. Ongoing research is exploring the interplay between trustworthiness and rapport in security vetting interviews, aiming to re-examine these dynamics within a context where rapport is of heightened significance.

In conclusion, trustworthiness and rapport emerge as pivotal factors in information-gathering efforts, exerting an indirect impact on information disclosure by shaping interviewees' willingness to trust and cooperate with the interviewer. While trustworthiness and trust have been overlooked in previous research, emerging evidence seems to suggest that they exert considerable influence on the quantity of information elicited. The nuanced interplay of trust and rapport remains subject to further exploration. For now, we advise practitioners to be aware of the impact their trustworthiness may have on information gathering outcomes and recognise that negative perceptions may not be adequately addressed solely through rapport-building efforts. Rather than attempting to address negative perceptions through subsequent actions, practitioners may pre-emptively avert such perceptions by actively demonstrating their trustworthiness early in interactions. However, further research is needed to determine the most effective approaches for enhancing perceptions of trustworthiness.

Lina Hillner is a third-year CREST-funded PhD Researcher. Twitter/X handle: @HillnerLina. Bluesky handle: @linahillner.bsky.social.

LORRAINE HOPE

NAVIGATING THE CROSS-CULTURAL CHALLENGES FOR EFFECTIVE RAPPORT AND INFORMATION GATHERING

Effective communication in cross-cultural interviews is crucial in an increasingly globalised world. By leveraging insights from experienced practitioners, new research explores how interviewers can prepare for successful rapport building and information gathering in cross-cultural interactions.

Even in domestic settings with increasing cultural diversity, the success of investigative interviewing and effective source handling hinges on adept information gathering practices. Building rapport, broadly defined as the quality of the connection between an interviewer and interviewee, is key for effective interviewing and associated with positive information-gathering outcomes. However, research on rapport in cross-cultural interviews is limited and misapplying the norms of one culture in another may not always fare well. While the fundamental impact of demonstrating basic humanity and authentic genuine consideration for an interviewee is likely universal, effective interviewers must be culturally competent to effectively build and maintain rapport, particularly when exploring sensitive topics in cultural contexts different to their own.

WHAT IS CULTURE?

Culture is a dynamic and intricate collection of shared systems, meanings, and practices within a social group. It arises from the group's history and experiences, influencing social interactions and relationships at all levels, from individuals to society. Cultural influence extends to cognitive processes, such as memory, and social processes, such as communication.

> **Anecdotal evidence suggests that cultural misunderstandings can lead to inefficiencies and frustrations being experienced by both parties during interviews.**

In investigative settings, the interactions between interviewees and interviewers can also be shaped by these cultural contexts, whether implicitly or more explicitly.

HOW MIGHT CULTURAL FACTORS MANIFEST IN RAPPORT BUILDING?

Investigative interviewing techniques typically originate from Western contexts, with limited consideration of cultural differences. While some research has examined the effectiveness of techniques in different cultures, few explicitly incorporate adaptations for cultural sensitivity. Anecdotal evidence suggests that cultural misunderstandings can lead to inefficiencies and frustrations being experienced by both parties during interviews.

Beyond cultural differences in memory accounts, which are reasonably well documented, differences in communication preferences are also likely to impact the progress of information-gathering interviews, including the development of rapport. Dominant theoretical frameworks accounting for communication preferences distinguish between low-context (usually more individualistic) and high-context (usually more collectivistic) communication cultures.

While individualistic cultures tend to prefer explicit, direct communication, collectivistic cultures tend to rely on indirect communication and contextual cues. In low-context communication cultures, relationships can be established quickly and get directly to the task. This is less likely to be a successful approach in high-context communication cultures where interviewers may need to spend more time on rapport-building efforts.

Relatedly, cultural differences in power distance (adherence to social hierarchy) and uncertainty avoidance (tolerance for unpredictability in social arrangements) likely impact communication dynamics during interviews, affecting rapport-building and the willingness of interviewees to express their views.

Honour culture, prevalent in various forms globally, adds another layer of complexity as the need to protect or maintain honour (or, in other contexts, 'save face') can influence the willingness of witnesses to disclose information, particularly for sensitive topics such as sexual assault.

Given this landscape of cultural differences, interviewers need to be adaptable and flexible when building rapport with the person in front of them.

HOW CAN INTERVIEWERS PREPARE FOR EFFECTIVE CROSS-CULTURAL INTERACTIONS?

In recent focus group research carried out with investigators experienced in conducting cross-cultural interviews, Hope and colleagues (under review) explored the perspectives of 66 practitioners concerning building rapport in interviews with people from diverse cultural backgrounds. Practitioners identified the importance of:

i. Careful interview preparation taking account of cultural norms and expectations.

ii. Being alert to the needs of the interviewee during the interview, which might present differently across cultures.

iii. Using communication informed by an understanding of cultural norms and preferences.

iv. Understanding the impact of social hierarchy in the interviewee's culture.

Practitioners also warned against applying the broad strokes of cultural expectation at the level of a single individual to whom they might not apply. They noted the additional challenges of conducting such interviews via interpreters or in less than fluent second languages.

These observations underscore the significance of cultural competence in interviewing. Cultural competence, well-established as a key educational component in other domains (e.g., healthcare), involves three main elements: cultural awareness (being aware of one's own ethnocentric beliefs and expectations), cultural knowledge (acquiring information about other cultures) and cultural skills/behaviour (possessing effective communication and behavioural skills for interacting with diverse people).

> **...cultural competence and adaptive rapport-based techniques are crucial.**

CONCLUSION

There is no one-size-fits-all approach for conducting cross-cultural interviews, but we know that cultural competence and adaptive rapport-based techniques are crucial. It is also worth remembering that best practices (e.g., open prompts, non-judgmental approach, non-leading questions) remain paramount. Simply put, the use of demonstrably ineffective interviewing methods such as hostility, leading questions, or failing to attempt to engage with an interviewee is unlikely to yield success in any cultural setting. And for effective rapport building, cross-cultural interviews, like all interviews, require a nuanced understanding of individual interviewee needs within their cultural context.

Lorraine Hope is professor of Applied Cognitive Psychology at the University of Portsmouth and a core member affiliated with the Information Elicitation programme of CREST.

VINCENT DENAULT & ALDERT VRIJ

"THE EYES CAN'T LIE": MISCONCEPTIONS ABOUT NONVERBAL COMMUNICATION AND WHY THEY MATTER

Security organisations are regularly offered techniques that claim to enable practitioners to predict hostile intents and threats through understanding 'body language'. Vincent Denault and Aldert Vrij discuss the efficacy of such approaches, the danger they may pose, and offer suggestions on how practitioners can distinguish the 'wheat from the chaff'.

Nonverbal communication typically refers to communication carried out in ways other than through words, including through nonverbal behavior. The subject has been addressed in thousands of scientific articles by a worldwide community of researchers in a variety of disciplines, including psychology, communication, and criminology. As well as academia, practitioners have shown interest in nonverbal behaviour, often as a means to increase their ability to understand others, even to spot liars. Security organisations are not spared. They are offered techniques to understand 'body language', which claim to allow the detection of hostile intents and threats through the observation of nonverbal behaviour.

Techniques to understand 'body language' have been around for thousands of years. In a 3000-year-old ancient sacred text, it was claimed that someone trying to poison others would show specific behaviour, including shivering, rubbing their great toe along the ground, and trying to leave the house. More recently, the public has been exposed to techniques of this nature via film and television. The examples are many. These includes the 1983 movie Scarface where Tony Montana, played by Al Pacino, claimed that "*The eyes, Chico. They never lie*," and the 1998 film The Negotiator, where Danny Roman, played by Samuel L. Jackson, claimed that:

> *"I'm reading your eyes. The eyes can't lie. Didn't you know what I was doing? A quick lesson in lying. You see, this is what us real cops do. We study liars. Example. If I ask you a question about something visual, like your favorite colour, and your eyes go up and to the left. Well, neurophysiology tells us that your eyes go in that direction because you're accessing the visual cortex. Therefore, you're telling the truth. If your eyes go up and right, then you're accessing the creative centres of the brain and we know you're full of s**t."*

With the advent of social media, the popularity of techniques to 'read body language' has been taken to a whole new level. 'Body language' experts receive a staggering amount of attention, with millions of views on social media. In a TikTok video viewed more than 9 million times since 2021, it is claimed that the direction of a person's gaze is a sign that someone is lying. In a separate TikTok video viewed more than 8 million times, Dr. Phil, an American TV personality, claims that the feet of liars "*will be pointed towards the door because they want out*"; akin to what was claimed 3000 years ago.

These claims are misconceptions about nonverbal behaviour. They are made even though decades of research has shown that nonverbal behaviour, including a person's gaze and feet direction, is unreliable for detecting lies in face-to-face interactions, that there is no Pinocchio's nose, and that misconceptions about nonverbal behaviour can result in severe consequences.

THE SEVERE CONSEQUENCES

When disseminated via traditional and social media, misconceptions about nonverbal behaviour may seem entertaining. However, when misconceptions about nonverbal behaviour, or techniques that promote them, find their way in the hands of people in positions of influence, they can result in severe consequences. For example, in law enforcement contexts, police officers trained in such techniques may be convinced (erroneously) that suspects are lying. They may close down other valid areas of investigation in favour of finding more information in support of their incorrect hypothesis that the suspect is guilty, thus wasting police time and resources. They may even allow themselves to use coercive interviewing tactics which

"Techniques to understand 'body language' have been around for thousands of years. But with the advent of social media, their popularity has been taken to a whole new level.

Image credit: © *Krakenimages.com edited by K.Brennan* | stock.adobe.com

can result in false confessions. In courtrooms, misconceptions about nonverbal behaviour can influence witness credibility and, ultimately, the judges' or jurors' decision. This can happen in various jurisdictions, and sometimes, misconceptions are integral to written judgments. An example comes from a Canadian court:

> *"Having carefully observed the accused during his testimony and noted his great nervousness, his fleeting gaze and his numerous hesitations in cross-examination, the court is convinced that [the defendant] has simply forged his version of the facts according to the evidence disclosed, and that he thereby lied to the court in a shameless manner"* (our translation)

However, law enforcement contexts and courtrooms are not the only places with a track record of using misconceptions about nonverbal behaviour. Security organisations are no exception. After 11 September 2001, the TSA (Transport Security Agency) set up the SPOT (Screening of Passengers by Observation Techniques) program to detect aviation security threats. However, when asked by the GAO (Government Accountability Office) to present the scientific evidence confirming the validity of the SPOT program, the TSA failed spectacularly. The TSA submitted 178 sources, but following an independent analysis, the GAO revealed that 175 of the 178 were irrelevant for assessing the validity of the SPOT program. The annual cost of the program was around $212 million. Despite this, the detection of hostile intents and threats through the observation of nonverbal behaviour is still ubiquitous within security contexts. A simple Google search for 'body language' and 'security' yields more than 19 million results, with a variety of security techniques being offered. The consequences of misconceptions about nonverbal behaviour should thus make distinguishing the wheat from the chaff a priority for organisations faced with safety and security issues.

"The consequences of misconceptions about nonverbal behaviour should thus make distinguishing the wheat from the chaff a priority for organisations faced with safety and security issues.

DUBIOUS CLAIMS AND FALLACIES

There is not a silver bullet to instantly assess the quality of these techniques, but some characteristics are relevant. The following may help you to identify whether a technique is worthy of exploring its integration into practice.

1.Beware those who claim that it is possible to 'read body language'

This claim is problematic as there is no such thing as a 'language' of the body. Face and body movements lacks characteristics of a formal language, including the absence of a vocabulary. The meanings of face and body movements are often ambiguous and are dependent on their context, including other verbal and nonverbal behaviours, the identity of the interactants, and the settings where they take place. There is no dictionary of face and body movements meanings.

2. Beware those who use science to establish their credibility, but then fail to do it in relation to their own techniques

For example, proponents of these techniques may say from the outset that face and body movements cannot be 'read' like words in a book. This is correct. They may even refer to 'science' and claim that there is nothing like a Pinocchio's nose. This is also correct. However, when presenting their techniques, they may then offer a variety of unfounded and discredited claims about nonverbal behaviour, including a myriad of facial expressions that, supposedly, can be monitored to gain insights on the psyche of others. In other words, science is useful to establish their credibility, but is disregarded when developing their techniques. At best, only parts of their techniques are based on scientific research, and typically, the evidence they consider is limited or disputed.

To give an example, a variety of 'body language' experts stress the importance of establishing a baseline (the "normal" behaviour of an individual) and then look for deviations. This advice appeals to common sense. For example, a person seems to be doing well, but after mentioning a certain subject, becomes silent and starts to cry. The deviation from 'normal' behaviour will draw attention.

"The meanings of face and body movements are often ambiguous and are dependent on their context, including other verbal and nonverbal behaviours, the identity of the interactants, and the settings where they take place.

However, in practice, it is very difficult, if not impossible to implement this advice. For how long should an individual be observed? Should all face and body movements be weighted the same? Is what is said considered? How is it considered? And when does face and body movement fall outside 'normal'? We further doubt the value of establishing a baseline, as stressed by 'body language' experts, because in the same situation, different people behave differently, but also, and perhaps more importantly, in different situations, the same person behaves differently. Finally, not only is the advice to establish a baseline often poorly explained, if not explained at all, but to our knowledge, there is no convincing evidence that it can be taught and applied to security practitioners.

Attention should also be paid to the paradigm of any experimental research that is used to provide evidence of the success of techniques to predict hostile intents and threats through understanding 'body language'. For example, when experiments are almost exclusively conducted with interviewees sitting in a room, findings cannot be directly applied to settings such as walking in an airport.

3. Beware the use of classic influence principles to sell the techniques

Some companies may use an appeal to authority. They will promote the name of their past clients, the fact that they have taught their techniques to various law enforcement agencies, or that they themselves were once part of one of these agencies. However, having taught or worked for the FBI, DEA or CIA is not proof of the efficacy of a technique, any more than having a celebrity endorsement is proof that a skin cream works. That a technique has been used for a long time also does not mean that it works. This is an appeal to tradition. Take Dr. Phil's claim that feet direction is a sign of lying. Finally, the reputation of a technique is sometimes highlighted with testimonials from satisfied clients. However, such testimonials are not proof of its efficacy. They are anecdotal evidence. People who use the technique may be biased towards noticing the hits (and ignoring the misses), which can lead to an overestimation of accuracy. Furthermore, testimonials from dissatisfied clients are rarely published.

IN SUMMARY: EXERCISE CAUTION!

People promoting questionable security techniques are probably doing so in all honesty, sincerely believing that they work. However, since these techniques are often based on misconceptions, they can result in severe consequences. And even if parts of the techniques are based on sound scientific research, the need for caution remains. This is why organisations faced with safety and security issues should be careful when opening their doors to techniques to detect hostile intents and threats through the observation of nonverbal behaviour. Beyond the points above that should prompt initial questioning, organisations should take the time to thoroughly evaluate what they are offered. There are several ways of doing this. One is to consider the UK's National Protective Security Authority guidance on behavioural detection, especially their checklist for measuring the suitability and effectiveness of techniques to detect hostile intents and threats. If they fail to exercise caution, organisations could be implementing techniques of no more value than those promoted by Al Pacino, Samuel L. Jackson and Dr. Phil.

Vincent Denault is a Postdoctoral Fellow at the Department of Educational and Counselling Psychology of McGill University (Canada). His research focuses primarily on issues related to nonverbal behaviour in justice and security contexts. Vincent is the co-founder of the Center for Studies in Nonverbal Communication Sciences and the co-founder of the Deception Research Society.

Aldert Vrij is a Professor of Applied Social Psychology in the Department of Psychology at the University of Portsmouth (UK). His research focuses primarily on issues related to nonverbal and verbal deception and lie detection. In 2016 he received the International Investigative Interviewing Research Group (iIIRG) Lifetime Achievement Award in recognition of his significant contribution to investigative interviewing.

DANA ROEMLING & JACK GRIEVE

FORENSIC AUTHORSHIP ANALYSIS

Despite the prevalence of written language in the digital age, forensic authorship analysis is an underestimated tool in forensic investigations, which can facilitate profiling authors and identifying authorship.

Imagine law enforcement is faced with a ransom note in a kidnapping case. One of the sentences in the note reads '*Put it in the green trash kan on the devil strip at corner of 18th and Carlson.*' You might notice that the author misspelt *kan* or that they correctly used *18th* and capitalised *Carlson*. This type of evidence could help you infer information about the author, although this can be tricky: It might seem like the author has a low education level, given this misspelling, but they spell other difficult words correctly, and may be trying to disguise their identity. Indeed, this is what was found to have happened in this case, while the feature that ultimately broke the case was the phrase *the devil strip*. This phrase is highly regionally bound and primarily used in the city of Akron, Ohio. This information was then used to narrow down the list of suspects.

This type of linguistic analysis is considered to be an application of forensic linguistics, specifically forensic authorship analysis. In general, authorship analysis is concerned with inferring information about the author of a document of questioned authorship. This could be:

a. to determine whether different texts were authored by the same individual, called *authorship verification*,

b. to assess who is the most likely author of a text given a set of potential authors, called *authorship attributio*n, or;

c. to infer characteristics about the author by their language use, called *authorship profiling.*

For example, authorship analysis has been used to assess whether a suspect had actually authored their police statements or to determine whether messages sent from a victim's phone were written by their suspected murderer. Limitations for authorship analysis arise through sparse data, genre constraints or texts being written by multiple authors. But, what features help determine the authorship of a text?

ANALYSING AUTHORSHIP

Even though, theoretically, every individual can use language in any way they please so long as they follow linguistic protocols (e.g., "grey green talk dog" is not a sentence that easily conveys meaning), people have preferences of how they use language. This means there is a degree of linguistic individuality, tendencies of using certain words with certain other words. Based on this assumption authorship analysis can generally assess whether texts were authored by the same individual. For example, in the Starbuck murder case the use of semicolons in a series of questioned emails was pivotal for showing that the emails were written by Jamie Starbuck who had murdered his wife, Debbie Starbuck, and then assumed her identity online.

The linguistic analysis found that he was impersonating her, but the usage of semicolons in the disputed emails was less clear at first. In their undisputed emails, Jamie used relatively few semicolons, while Debbie used them with great frequency. In the disputed emails, semicolons were used far more frequently than had even been observed in Debbie's writing. Further examination, however, revealed that the semicolons in the disputed texts were used grammatically in the same way as Jamie, as opposed to Debbie. It was therefore concluded that Jamie had purposely increased his rate of semicolon usage to impersonate Debbie, but had not appreciated the grammatical pattern that characterised Debbie's usage, thereby revealing himself.

> **Jamie had purposely increased his rate of semicolon usage to impersonate Debbie.**

REGIONAL PROFILING

When there is no comparison material, authorship analysis can still provide important insights into the author of a text. Authorship profiling focuses on the linguistic features that let us predict the social characteristics of an author, for example, age or gender. This type of analysis is rooted in sociolinguistics, the analysis of language and its relationship to society. In dialectology, for example, sociolinguists research the regional distribution of language variation. This research can then be applied to forensic authorship questions and be used for regionally profiling an unknown author, which is an exciting area of current research.

> **Authorship profiling focuses on the linguistic features that let us infer characteristics of an author.**

Profiling the regional background of an author can be done through careful, manual analysis and requires the analyst's knowledge about regional dialect variation, as illustrated in the ransom note example above. This task, which is referred to as geolinguistic profiling, can also be based on statistical or computational methods, for example, comparing the language used in an unknown text to patterns of regional variation observed in large collections of social media data.

This is a topic we are currently working on, developing a method for automatically profiling the regional background of the author of a questioned document through the quantitative analysis of large corpora of English and German social media data. Specifically, our approach involves creating a map for each word in a questioned document showing its regional distribution. These maps can be combined into one map, weighing each word map by its regional strength. An aggregated map like this shows how language used on social media would predict the location of the analysed text and could aid law enforcement in their investigations.

Interested practitioners can find more information on forensic linguistics and contact details of forensic linguists through the global forensic linguistics mailing list (http://bit.ly/mail_fl) and the International Association for Forensic and Legal Linguistics (IAFLL.org).

Dana Roemling is a doctoral researcher at the University of Birmingham. Their PhD research focuses on Geolinguistic Authorship Profiling, and they are interested in Authorship Analysis, Language and Law and Lavender Linguistics.

Jack Grieve is a Professor of Corpus Linguistics at the University of Birmingham. His research focuses on Dialectology, Authorship Analysis, Computational Sociolinguistics and Language Change.

Image credit: © *Donatas Dabravolskas* | stock.adobe.com

BECKY PHYTHIAN

LAW ENFORCEMENT INFORMATION SHARING FOR THE 21ST CENTURY

Effective law enforcement practice requires the identification — and communication — of relevant and timely information. How is this currently done and how can it be improved?

THE BACKGROUND

Intelligence-led policing (ILP) uses intelligence to inform decision-making and direct law enforcement activities, and emerged in the 1990's as agencies realised a more targeted approach was needed to tackle offenders and reduce crime. However, the criminal landscape was transformed in the 21st Century as globalisation and technological advances have allowed offenders, commodities and information to travel physically and virtually with greater ease. Crime has become increasingly transnational.

It remains difficult for offenders to commit crime without leaving physical and electronic traces. These traces can be captured in various ways, including diverse camera systems (e.g., CCTV, ANPR), banking transactions, and communication mediums (e.g., texts, social media). However, capturing relevant and timely information is no easy task when it's held in different regions and countries, by different agencies, in different formats and on different systems. Multiple public inquiries worldwide have criticised law enforcement communication and intelligence failures, whereby critical information has not been communicated with partner agencies (or in a timely manner) and has resulted in the failure to prevent or effectively respond to an incident. Globally, billions of pounds have been spent in response (e.g., developing new agencies or technology), yet the problem persists.

> **…capturing relevant and timely information is no easy task when it's held in different regions and countries, by different agencies, in different formats and on different systems.**

Previous studies to explain barriers to information sharing have highlighted culture (i.e., trust), procedure (i.e., sharing protocols and legislation) and technical issues (i.e., incompatibility, cost). However, this insight has remained at a general level, generated from the assumption that information sharing is conducted in the same way, no matter what agency or information is involved.

INTERNATIONAL LAW ENFORCEMENT INFORMATION EXCHANGE

My UK Research and Innovation Future Leaders Fellowship looks to test some of these assumptions by exploring how international law enforcement agencies exchange information (www.ilex.ac.uk). Initially focusing on the UK, our research has established that the type of information being exchanged (i.e., tactical vs strategic) and the information recipient (i.e., outside the agency peer group such as an international entity or NGO) influences the nature of communication. Four ways in which information is shared, from most to least used are:

i. **Inform and request:** an agency representative will (formally or informally) highlight information and ask whether another agency has further information.

ii. **Meet and share:** an information sharing partnership is created between trusted and invited agencies. Here representatives meet (physically or virtually) to provide information on subjects of mutual interest while maintaining exclusive access to their systems (i.e., Multi Agency Safeguarding Hubs).

iii. **Customised database:** collaborating agencies use a bespoke database to pool information. Such systems are isolated from other organisational operating systems and enable partners to interrogate the information however they wish (i.e., the organised crime group mapping system).

iv. **Integrated systems**: an agency can directly view, in real time, another agency's data/system – or part of it (i.e., the Police National Database [PND]).

My research has revealed that an 'inform and request' approach, despite being used most, is least effective and efficient as it is resource intensive and personality driven. In contrast, an 'integrated systems' approach was the least frequently used even though the technology exists to link diverse databases and use algorithms to automatically flag criminal patterns and active offenders. Yet, despite being the purest approach to multi-agency working, practitioner reluctance remains to sharing information in this way. These findings appear consistent in Australia too.

> **How can offenders who exploit the jurisdictional ownership and diverse information silos of fragmented law enforcement agencies be more effectively and efficiently tackled?**

THE IMPORTANCE OF THIS RESEARCH

Stock mirrors the concerns of many commentators when he highlights the current "global security crisis" associated with an "epidemic of transnational organised crime". How can offenders who exploit the jurisdictional ownership and diverse information silos of fragmented law enforcement agencies be more effectively and efficiently tackled? There appears significant scope for law enforcement agencies to improve information management. The technology exists to integrate systems to provide a more holistic understanding of crime patterns and offender behaviour. They also reduce administrative burden (i.e., double keying) while maintaining security (i.e., access, audit trail), enabling agencies to determine which information to access and analyse, how and when. Information is communicated almost instantaneously. The PND is an example of this. Yet, despite the benefits of the system and its capabilities being recognised, it's not used to its full potential and practitioner hesitancy remains. This emphasises the importance of considering all aspects of this process (i.e., cultural change and technology implementation), as well as the need for evidence to inform policy and practice to ensure investment and resources are used in the most beneficial and productive way.

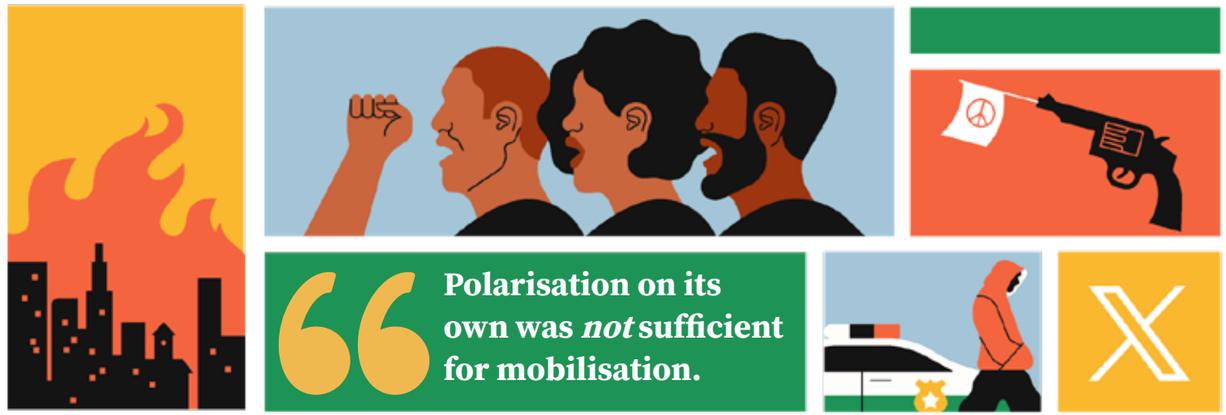
Dr Becky Phythian is a Reader in Policing at the School of Law, Criminology and Policing at Edge Hill University, and a UKRI Future Leaders Fellow exploring international law enforcement information exchange. Her Twitter (X) handle is: @beckyphythian.

Image credit: © *Moon Project* | stock.adobe.com

LAURA G. E. SMITH

DIGITAL TRACES OF OFFLINE MOBILISATION

By integrating data-driven methods with psychological theory, we provide responsibly developed tools to model the relationship between social media activity and participation in offline collective action.



THE DYNAMICS OF MOBILISATION IN THE DIGITAL AGE

We are in an age of protest. From the anti-Brexit 'People's Vote' marches of 2018, to the Black Lives Matter protests of 2020, to the pro-Palestine marches of 2023 and 2024, collective action has surged to unprecedented levels. In recent years, we've witnessed a significant increase in the mobilisation of collective action worldwide, spanning peaceful mass protests to violent extremist action. This surge coincides with the global expansion of internet users, surpassing five billion, including 4.95 million social media users. Concurrently, we have witnessed collective action taking many forms, and occurring both online and offline: for example, online people can post information about social causes, as well as symbols of unity and allyship, recruit new members to their group, crowdsource Distributed Denial of Service (DDoS) attacks, and hack rival organisations.

The online and offline worlds are not separate: people can communicate online whilst engaging in offline action, and vice versa. These social media interactions, sometimes dismissed as trivial, are instrumental in the mobilisation of collective action. Social media serve as spaces for debate, disagreement, and the expression of opinions on social injustices, fostering a sense of shared values among individuals. Indeed, it's been suggested that the internet is the 'greatest critical enabler' for mobilisation: but is there any evidence that people mobilise, at least partially, through their online communications? If so, what are the implications of using online communications data to predict future mobilisation? What ethical considerations arise from developing tools to analyse people's digital footprints for this purpose? Is the internet 'the greatest enabler' of mobilisation?

There are several reasons why communicating via networked technologies might facilitate mobilisation. Social media aid in the development of social groups and networks, providing a platform for online communication of grievances that may lead to polarisation and radicalisation. The internet's capacity for rapid information dissemination and logistical planning further enhances its role in organising, advertising, and serving social-psychological functions in mobilising offline collective action.

Politicians and policymakers have emphasised the role of online polarisation in motivating individuals to join and participate in radicalised groups, which is crucial for collective action. Indeed, in the wake of an increase in extremist action in which social media sites were implicated, politicians took legislative steps to prevent people from becoming radicalised on social media platforms (e.g., the U.K. Online Safety Act 2023). Online polarisation has been cited as a risk factor for mobilisation to violence in the United Kingdom's and Australia's counterterrorism strategies. However, there is a lack of specificity in the claims around how and why online polarisation might cause offline mobilisation, and there are no established methods to capture the polarisation of individual users in communications data - and therefore no evidence that directly links an individual's online polarisation with their offline behaviour. This means there is room for a more granular understanding of the connection between people's online behaviour and their offline participation in collective action.

> **The internet facilitates the rapid communication of information and enables the planning of logistics.**

The relationship between online interactions and offline collective action is intricate. While online interactions commonly encourage offline activism, some research suggests they can also have a *demobilising* effect, satisfying the need to act offline, or people may even have disingenuous motivations for engaging in them. These latter online collective actions may be examples of 'performative' allyship, which have no significant disruptive offline impact.

THE DIGITAL TRACES OF MOBILISATION

Digital traces are digital records of online activities and events, offering valuable insights into the connection between online and offline behaviors. To understand and predict how and why people's online interactions may be related to their offline mobilisation, we modelled the digital traces left by people engaged in and discussing the anti-Brexit 'People's Vote' marches.

The People's Vote March, a significant rally against Brexit, unfolded on October 20th, 2018, drawing an estimated 700,000 participants in London. Online groups formed to encourage people to attend the march, and on social media there was widespread political polarisation, which had an economic fallout and was accompanied by a rise in hate crime. This context provided us with an opportunity to investigate how people's online behaviour and offline collective action intersected.

We developed new methods to enable us to test and potentially improve the predictive capabilities of psychological theories of collective action, so that we could better explain *why* online communications could predict offline mobilisation. Conversely, we used psychological theories to inform the design of our algorithms to enhance the algorithms' rigor, validity, and effectiveness.

KEY TAKEAWAYS

1 Online polarisation did not predict mobilisation

Our research modelled online polarisation as *communication behaviour*, employing an equation capturing changes in people's online communications data (as a relative intensification of an individual's posts about a grievance over time). We found polarisation on its own was *not* sufficient for mobilisation.

2 Validation from others matters

The impact of online polarisation on mobilising individuals for the People's Vote March depended on the validation (likes) received on their Brexit-related posts. This validation served as a cue, affirming and validating shared perceptions of injustice and fostering a sense of group support. That provided a solid psychological foundation for taking offline action.

3 People leave a digital footprint of mobilisation

We found that in the 24 hours around the protest event, people left an online 'digital footprint' of their participation in offline collective action. Therefore, the digital traces left online by people before and during an offline protest event can indicate that they are, or will be, attending that event.

4 Enhancing security through digital traces

The algorithms could be employed to (a) detect potential unrest, (b) provide information to first responders about the potential size of crowds at protest events, and (c) therefore inform crowd management strategies prior to and during large-scale events.

> **In the 24 hours around the protest event, people left an online 'digital footprint' of their participation in offline collective action.**

5 Balancing risks and benefits

Algorithms predicting lawful protest pose potential ethical concerns. Our results should be used to safeguard rather than limit lawful protest mobilisation.

Individual's motivation and self-efficacy for engaging in collective action likely originates online before translating into real-world actions. However, expressing grievances online does not necessarily imply dangerous intentions on an individual level, although it might inspire others. Instead, social media sites act as catalysts for mobilisation, providing spaces for validating grievances and ideas. Rather than censoring expressions of grievances online, which may stifle positive social change, policy should focus on social media sites' algorithms, affordances, and features that drive people together and enable them to validate and legitimise unlawful, violent extremist ideas.

This text is adapted in part from a research article (see Read More).

Laura G. E. Smith is a Professor of Psychology at the University of Bath and co-Director of the Bath Institute for Digital Security and Behaviour, and Lead of the Digital Lives lab.

LAURA M. STEVENS, TIA BENNETT, SARAH ROCKOWITZ & HEATHER D. FLOWE

THE ROLE OF DIGITAL TECHNOLOGIES (GBVXTECH) IN DOCUMENTING GENDER-BASED VIOLENCE

New digital technologies are being used for victims to communicate their experiences of gender-based violence to law enforcement and other agencies. However, these technologies are not considering minimum best practice principles for interviewing victims face-to-face.

Gender-based violence (GBV) is a global issue that disproportionately affects women and children, with 1-in-3 adult women and 1 in 2 children worldwide having experienced domestic and/or sexual violence within their lifetime. Concerningly, the actual prevalence rates of GBV may be much higher due to mass under-reporting. For example, only one-sixth of all sexual offences are reported to the police in the UK and only 1.6% of those cases result in a conviction. As such, there has been a global movement to document cases of GBV using alternative formats (e.g., digital platforms).

> **GBVxTech must align with established minimum best practice standards for gathering victim accounts to collect the strongest evidence for investigations and prosecutions.**

#METOO AND THE DIGITAL REVOLUTION

Given the global pandemic that is GBV, the #MeToo movement went viral in 2017. The movement was initially started to support women of colour in disclosing sexual violence, but later to provide all victims of GBV with a space to document their experiences on social media. Following its inception, the hashtag MeToo was used over 19 million times within the first year, which reveals the mammoth nature of GBV globally. From this movement, we have seen a growth in mobile phone applications and online platforms to assist in gathering evidence and reports from all victims of GBV.

GBVXTECH - WHY IS IT USEFUL?

GBVxTech platforms allow victims to disclose incidents soon after they occur. In this way, GBVxTech captures critical memory evidence before the amount and specificity of recall decreases over time. If and when a victim later decides to involve authorities, a detailed account can aid the investigation and prosecution. Given that a victim's statement is frequently the central evidence in GBV cases, tools that facilitate thorough, timely documentation of the victim's account offer major benefits for justice. GBVxTech must align with established minimum best practice standards for gathering victim accounts to collect the strongest evidence for investigations and prosecutions.

GBVXTECH - DOES IT ALIGN WITH MINIMUM STANDARDS OF BEST PRACTICE?

To investigate whether GBVxTech platforms adhere to the best practice principles recommended for face-to-face interviews, we conducted a systematic review of all GBVxTech we could access (N = 13) that documented a disclosure from a victim. We found that almost all of the GBVxTech platforms reviewed used open questions at least once, encouraged the victims to report their account in their own words without influence from others, and asked crime-relevant questions imperative to facilitate investigations, which is all in line with best practice. Positively, none of the platforms reviewed asked leading questions. However, the most commonly used responding method was forced-choice drop down menus. These limit the amount of detail a victim is able to communicate and may invalidate the victim if they feel that their experience is not captured within the options provided.

Digital GBVxTech platforms cannot replicate all aspects of in-person interviews. However, key best practices could be implemented in these platforms to enhance disclosure quality and minimise re-traumatisation.

For example, GBVxTech currently lacks a pre-interview phase. Ground rules could be provided, instructing victims to report unsure details. Narrative practice could be included, allowing victims to first recall a neutral event. Studies show such ground rules and narrative practice facilitate accuracy by setting expectations. A short pre-interview stage on GBVxTech could administer these techniques before questions on the incident. Simple additions like these, drawn from research on optimal interviewing, can improve complete and accurate documentation without necessitating face-to-face interaction.

> **Moving forward, alternative communication platforms like GBVxTech must prioritise victim safety and confidentiality above all else.**

RECOMMENDATIONS FOR THE FUTURE

Where possible, GBVxTech platforms should adhere to minimum standards of interviewing best practice to allow victims to communicate their independent voice and document their most complete and accurate statement. But there are additional challenges that come from using alternative digital reporting methods. For example, it is recommended that GBVxTech platforms are accessible for all; but, all the platforms we reviewed require a smartphone with WiFi or a data connection to document a case. Therefore, future GBVxTech platforms should consider how to provide offline reporting for individuals who do not have data privileges. Additionally, current GBVxTech platforms are not accessible for individuals with visual or cognitive impairments to communicate (e.g., text-to-speech functions). GBVxTech providers should partner with accessibility organisations to ensure all individuals can communicate their experiences.

Furthermore, and our most concerning finding, around only half of all the platforms we reviewed had security features (e.g., password protection) to ensure that the victims' reports were safe and could not be viewed by anyone who can access their phone (e.g., the perpetrator in intimate-partner situations). Moving forward, alternative communication platforms like GBVxTech must prioritise victim safety and confidentiality above all else.

Laura Stevens is a final year PhD student at the University of Birmingham, supervised by Professor Heather Flowe and Dr Melissa Colloff. Tia Bennett is a third year PhD student at the University of Birmingham working with Dr Melissa Colloff and Professor Heather Flowe. Sarah Rockowitz, MSPH, MSc, is a PhD candidate in the School of Psychology at the University of Birmingham. Heather Flowe is a Professor of Psychology at the University of Birmingham in the UK.

ANASTASIA KORDONI, SHENGNAN LIU, MIRIAM KOSCHATE-REIS & MARK LEVINE

INVESTIGATING THE INFLUENCE OF HYBRID SOCIAL IDENTITIES IN ONLINE COMMUNITIES

With hybrid identities becoming an increasing feature of online communities, we explored the adaptive capacity of these identities through language and showcased their influence potential for online extreme communities.

WHAT ARE HYBRID IDENTITIES?

People belong to many social groups, such as religious, gender, professional. These affiliations shape how we see ourselves and guide our actions, aligning our behaviours with the beliefs, values, and norms of the groups we identify with. According to the Social Identity Approach, our influence within a group is rooted in appealing to our shared group membership. In the digital realm of online communities, the same dynamics apply. Online communities emerge from people who have the same identity founded on shared belief systems. Yet, there is an increasing trend in the formation of online communities with not a distinct but rather a hybrid identity.

> **A hybrid identity is defined as the fusion of two distinct group memberships and their corresponding belief systems.**

A hybrid identity is defined as the fusion of two distinct group memberships and their corresponding belief systems. This phenomenon is on the rise and can include different types of identity mutations. For example, a feminist parent can be a hybrid identity if beliefs associated with both identities, the feministic and the parent, are intertwined in ways that shape certain kinds of behaviours. This formation of a hybrid identity has recently become prevalent in extreme online communities, such as right-wing extremist communities. For example, an eco-fascist identity can be seen as a prominent hybrid identity, where the 'eco' identity echoes the belief system of environmentalism and the 'fascist' identity appeals to populist and far-right belief systems.

The potential impact of these hybrid identities is evident in recent violent events. For example, eco-fascist ideas have been implicated in the 2019 Christchurch incident and the 2022 Buffalo supermarket attack. The possibility of such security threats necessitates a comprehensive investigation into the mechanisms through which hybrid identities can exert influence online.

HOW CAN WE EXPLORE THE INFLUENCE OF A HYBRID IDENTITY?

We can explore the influence potential of a hybrid identity through the computational analysis of language. As Hernández-Campoy indicated, language is a perfect tool for expressing social identities because language acts are themselves acts of identity. In this sense, language is the ideal behaviour to study how hybrid identities can be communicated to influence other online communities. Our project explored hybrid identities using the eco-fascist identity as a case study. We collected text data from social media forums to investigate whether a hybrid identity does indeed include linguistic characteristics of both identities or it is a merely distinct form of identity.

> **...language is a perfect tool for expressing social identities because language acts are themselves acts of identity.**

Through the lens of natural language processing, we quantified a list of linguistic features that reflect how people who hold specific identities (ecological, far-right or hybrid) talk or write rather than the content or topic of the discussion. These features were then used to train and test an Automated Social Identity Assessment (ASIA) model for hybrid identities. This model can detect which identity is situationally salient based on users' writing style. In this way, we could test whether linguistic features of the ecological and far-right identities co-existed in the hybrid identity.

As we put the ASIA model to the test on the hybrid forums, the results demonstrated that the data from these forums embodied linguistic features of both identity types. Further analysis showed that it wasn't merely a blend of identities but a dynamic interplay, revealing the adaptive capacity of the hybrid identity. Our analysis indicated that the hybrid users' writing style was more reflective of the ecological identity in ecological threads and transitioned into linguistic features that were more reflective of the far-right identity in far-right oriented threads. Switching between these identities, namely adapting to the socio-linguistic style of the salient identity as a means of influence can be hard to challenge.

CONCLUSIONS

These findings shed light on the online resilience of extreme groups showcasing the role of hybridity as a means of linguistic adaptation to forum requirements, such as the topic of a thread. Our project delves into the realm of hybrid identities revealing a capacity to dynamically adjust communication styles based on the context in which they are expressed — marking a shift in our understanding of online influence. It is this very adaptive capacity that painted certain hybrid identities, such as the eco-fascist identity as resilient, namely an identity that weaves itself into diverse discussions.

In that sense, shifts in identity salience and writing behaviour may pose a risk of spreading far-right ideological positions into more mainstream online communities. Our project is the first step towards comprehending the dynamics of online hybrid communities and their influence on our collective social landscape. Future research is needed to unravel the mechanisms and consequences of such hybrid identity influences. This can combine natural language processing techniques with experimental and qualitative work to a closer examination of the trajectory of hybrid identities — a step towards mitigating potential risks and fostering a more nuanced understanding of the communicative means of this evolving socio-digital phenomenon.

Anastasia Kordoni is a Senior Research Associate at Lancaster University. Shengnan Liu is a Senior Research Associate at Lancaster University. Miriam Koschate-Reis is an Associate Professor for Computational Social Psychology and Deputy Director for IDSAI at the University of Exeter. Mark Levine is a Professor of Social Psychology at Lancaster University.

MARC KYDD, LYNSAY SHEPHERD, GRAHAM JOHNSON & ANDREA SZYMKOWIAK

LOVE BYTES:

IMPROVING ROMANCE FRAUD PREVENTION

Romance fraud has substantially increased over the past decade. Traditional preventative and support measures have struggled to keep up with this form of cybercrime, suggesting a more personalised prevention approach is needed.

A UNIQUE FORM OF FRAUD

Online romance fraud, whereby a scammer feigns romantic interest in a user of a dating platform to financially exploit them, has surged in recent years. In the US, reported losses have reached $750 million annually, while in the UK, losses have totalled almost £100 million in the past year. These figures may be conservative, as romance fraud is often under-reported due to the embarrassment victims suffer.

Romance fraud goes beyond being a financially devastating cybercrime; it also carries a significant emotional toll. Victims not only experience financial loss but also grapple with the emotional impact of realising that what seemed like a genuine relationship was a scam, with many struggling to accept the fact they have been exploited. The emotional impact often prevents many victims from seeking support due to the feeling that being scammed is a personal failure; others suffer a breakdown in the trust of others.

A CHALLENGING FORM OF FRAUD

While prior work has focused on analysing meta-aspects such as profile pictures and user bios for scammer-traits, research into how technology solutions can be integrated into the design and application of warnings against romance fraud is limited.

As scammers often tailor their approach, each victim receives a 'personalised love story'. Thus, the awareness campaigns seen most frequently around Valentine's Day, such as TakeFive, often fail to offer targeted, actionable messaging. For example, the TakeFive advice doesn't consider scammers who deploy 'foot-in-the-door' or those who may request photos/videos for later use in sexploitation. Meanwhile, international attempts to raise awareness and standardise messaging, such as the inaugural World Romance Scam Prevention Day, are still in their infancy.

Below, we explore current preventative and supportive measures for victims of romance fraud and argue that a personalised approach is merited to tackle the issue.

Preventative Measures

Awareness campaigns can help users defend themselves against scammers before they become a threat in the form of a simple, easily distributable means of warning about the risks of romance fraud. By highlighting common scammer tactics, users can, in theory, apply the message to their situation. However, awareness campaigns must be generalisable to different scenarios. This creates the issue of 'white noise' whereby users can be confused about what constitutes romance fraud, with victims failing to see their experience reflected in the messaging.

If users cannot find relevant information through awareness campaigns, they may turn to self-education in the form of online searches. This rudimentary approach poses new challenges.

> **…in the UK, losses [to romance fraud] are placed at almost £100 million in just the past year.**

Given the often-explicit nature of romance fraud in the form of sextortion and blackmail, some users have found that some relevant materials were blocked by their Internet Service Provider – being mistaken for indecent material, due to the keyword searches of 'sextortion' or 'revenge porn' used. In other cases, materials in proprietary file formats cannot be accessed by all users, or links to materials are no-longer available.

Supportive Measures

For victims of romance fraud, peer support groups offer tailored face-to-face advice. While peer support groups are an important first step for victims on the road to recovery, they are not without issue. Although attendees receive in-person peer support groups positively, continued attendance did not reflect this. As many as 90% of attendees were no longer attending sessions one year on from their first visit. Victims noted the discomfort that comes from being open about extremely private conversations and many opted to listen to others instead. The lack of engagement with the group led some to stop attending, creating a feedback loop where a small group of victims becomes even smaller as more and more no longer attend.

An approach to mitigate the financial damage is reporting cases of romance fraud to the authorities. Correia studied how Action Fraud, the UK's national fraud reporting centre, recorded reported data, suggesting that various pieces of information were either missing or misreported, such as which investigator was assigned to a case, or the amount of money lost in a scam. In cases where victims were exploited of smaller amounts of money over a longer period, it may not be initially clear just how much has been lost and as such the total amount lost was recorded as '0'; making it harder to determine the severity of the crime. Broader demographic information, such as age, ethnicity, and background, were also not recorded. Failing to record which communities are affected by romance fraud makes it more challenging to create effective outreach programs tailored to minorities who also experience romance fraud.

A PREVENTABLE FORM OF FRAUD

The above overview illustrates that current approaches are not meeting the needs of users – both in terms of preventing romance scams and supporting victims. Existing methods simply do not have the speed and flexibility to adapt to the scammers ever-evolving playbook – perhaps a critical rethink of tackling romance fraud using a technology or data driven approach may be needed.

While it is encouraging to see users taking proactive steps in the form of self-education (Ibid.), there should be a more curated approach, for example, in the form of a central repository of information. The issues raised around the generic nature of awareness campaigns also suggest that the user's own context should play a more significant role in the advice provided through conversational analysis – using the likes of AI; consideration should be given to directly integrating warning systems with dating platforms such as those on banking apps.

> **Despite the devastating impact of romance fraud… implementing effective countermeasures against such crimes continues to prove difficult.**

Building safety measures into dating platforms can protect users from harm, using real-time safeguards. Our work in deploying AI-backed safety measures that operate as the user converses with the potential scammer removes the need to remember potential warning signs. Instead, they are alerted to suspicious activity as it occurs. While still in the developmental stage, our work shows promising signs of moving romance scam prevention in a more dynamic, responsive, and, hopefully, effective direction; helping keep users safe regardless of the scammer's tactics.

Romance fraud is a complex and evolving cybercrime. Safeguards deployed against it should be equally adaptive to users' needs. By exploring countermeasures that integrate with dating platforms directly, a more flexible approach can be taken to inform, educate, and protect users.

Marc Kydd is a PhD student working on Machine Learning and Usable Security. Dr Lynsay Shepherd is a Senior Lecturer in Cybersecurity and Human-Computer Interaction. Prof Graham Johnson is Professor of Human-Centred Technology. Dr Andrea Szymkowiak is a Senior Lecturer in Human Computer Interaction. The research team are based in the School of Design and Informatics at Abertay University, Dundee.

Image credit: © *Pawel Czerwinski* | unsplash.com

NADINE SALMAN & ZAINAB AL-ATTAR

NEURODIVERGENCE & EXTREMISM: CONSIDERATIONS FOR PRACTICE

A summary of findings from three studies examining the contextual relevance of neurodivergence within extremist populations and subsequent considerations for practice.

Existing research does not indicate that neurodivergence (e.g., autism and ADHD) causes extremism engagement in the general population. However, while estimates vary, a proportion of individuals within extremist populations are neurodivergent. These individuals may follow a different pathway to engagement and have different needs than their neurotypical counterparts.

Here, we summarise the key findings from our research (see read more) and considerations for practice

1 RESTRICTED INTERESTS

Neurodivergent extremists may develop specific intense interests that draw them into and keep them engaged in extremism. While these intense interests may serve psychological functions for the individual (e.g., alleviating stress), they may become associated with harmful subjects, including terrorism. According to our research, harmful interests may arise from precursors such as military history, especially the Second World War; mass murder and violence; weapons (firearms, knives, and bombs); computers and technology; extremist narratives or ideologies; conspiracy theories; and politics. Technical and weapon-related interests may confer criminal capability (e.g., bomb-making), while multiple interests may converge to shape risk.

2 VIVID FANTASY AND IDEATION

At-risk neurodivergent individuals may experience vivid extremism-related fantasies and ideation. In our research, this included detailed visual fantasies depicting violent ideation or preoccupations with death – usually inspired by existing violent imagery viewed online. Violent ideation may be associated with intense interests, and often appeared to redress feelings of anger, distress, and injustice. These fantasies can extend to idealised versions of themselves, contributing to a grandiose narrative surrounding them and their actions. In some cases, particularly where individuals become desensitised to violent imagery, they may transition from fantasy to action.

3 OBSESSIONALITY, REPETITION, AND COLLECTING

Interests may become obsessive and include the collection of associated items, images, or videos. In our research, this included collections of weapons, Nazi memorabilia, and virtual content such as memes, propaganda, and violent videos. These collections may provide opportunities for detection, or in extreme cases, grounds for conviction. As well as obsessively pursuing their interests, at-risk individuals may demonstrate a fixation, preoccupation and repetitive thinking and communication linked to specific grievances or feelings of injustice.

4 SOCIAL INTERACTION AND COMMUNICATION DIFFICULTIES

Social and relationship difficulties experienced by neurodivergent individuals may lead to isolation, feelings of resentment, and personal grievance. This may, in combination with other factors, fuel revenge fantasies and identification with extreme ideologies that offer an explanation or social status. Social difficulties may push individuals to retreat into online communities, where they can communicate about their interests and may feel more competent and connected, but may be exposed to more extreme content and actors.

Image credit: © *SB Stock edited by R.Stevens CREST* | stock.adobe.com

> **Neurodivergent cognitive styles can be seen both as strengths and potential difficulties.**

A lack of social awareness may also lead individuals to 'leak' their extreme views, resulting in referrals to authorities.

5 NEED FOR ORDER, RULES, ROUTINES, AND PREDICTABILITY

Autistic individuals may have a need for predictability, order, structure, rules, and routines. Changes to routines or perceived loss of order can be associated with stress and frustration that may contribute to grievances. 'Rule-based' ideologies that claim to restore order may be attractive to at-risk individuals.

6 COGNITIVE STYLES (STRENGTHS AND DIFFICULTIES)

Neurodivergent cognitive styles can be seen both as strengths and potential difficulties. There may be a tendency to overfocus on minute details (of an interest, or a fixation on a grievance) while overlooking the bigger picture and context. This could lead to a lack of consideration of the consequences of their actions. Information that is presented in the form of facts, categories, fine details, and patterns, may resonate and have a pull. Difficulties in organisation, planning, and prioritisation may exacerbate professional and academic challenges faced by individuals that may contribute to grievances. Impulsivity may be linked to impulsive risk-taking behaviour and violence.

7 SENSORY NEEDS AND SENSATION-SEEKING

Over-sensitivity to sensory input may contribute to difficulties in school or work and subsequent isolation, and may drive some individuals to self-soothe through risky interests and online spaces. It may also lead to a perception of the world as threatening.

Meanwhile, under-sensitivity may be expressed through sensory-seeking behaviours, including interests in violent video games, fire, explosions, weaponry, and shooting. Elaborate stimuli may have a strong pull. Individuals may experience desensitisation from repeated exposure, leading them to seek more extreme content and engage in riskier behaviour.

8 COMPLEX NEEDS AND COMORBIDITIES

Additional factors often interact with or exacerbate difficulties associated with neurodivergent symptoms, creating complex and interacting needs. In our research, this included other diagnoses (e.g., other neurodivergence, schizophrenia, depression, and anxiety), trauma (e.g., experiences of abuse), and other life stressors (e.g., familial, relationship, and employment difficulties). These can be exacerbated by a lack of support services and transition periods, such as the transition to adulthood. Such difficulties can drive individuals to self-soothe through their risky interests and behaviours.

CONCLUSIONS: ENHANCING RESILIENCE AND CONSIDERATIONS FOR PRACTICE

Overall, our findings suggest that some neurodivergent features can contextualise extremism vulnerability and risk, but rather than directly causing this risk, they can become a context for push and pull factors linked to extremism and combine with or exacerbate other vulnerabilities. Within populations of concern, risk assessment approaches and interventions may benefit from considering how specific neurodivergent traits and symptoms can contextualise risk, vulnerability, and resilience, and their interaction with other factors.

Practitioners may benefit from:

- Adopting tailored neurodivergent-friendly approaches
- Harnessing protective factors, including leveraging strengths conferred by neurodivergent features
- Considering wider environmental and systemic factors such as school, mental healthcare, and social support
- More in-depth and practical training to guide them through understanding neurodivergent needs and the complex implications they may have for assessment and interventions.

Nadine Salman is a Senior Research Associate at Lancaster University. Twitter/X: @Nadine_Salman. Professor Zainab Al-Attar is a Senior Lecturer at the University of Central Lancashire, Honorary Research Fellow at UCL, and Adjunct Professor at Victoria University, Australia.

AUSTIN DOCTOR, GINA LIGON & SAM HUNTER

MILITANT LEADERSHIP AND THE SEVERITY OF TERRORISM IN CONFLICT ENVIRONMENTS

The NCITE team explores whether militant leaders' exposure to violence predicts their tactics and strategies on the ground.

On 7 October 2023, Palestinian terrorist organisation Hamas initiated Operation Al-Aqsa Flood, a series of coordinated attacks against multiple Israeli civilian and military targets. In the first day, approximately 1,000 Israeli civilians and more than 350 Israeli soldiers were killed. The operation drew the public support of aligned militant groups in the region, including the Lebanese terrorist organisation Hezbollah. With unsubtle reference to the Beirut Bombings that killed 241 U.S. service members in the 1980s, Hezbollah leader Hassan Nasrallah seemed to directly address American political and military officials in recent public speech, stating "Your fleets in the Med do not scare us...We have prepared a response to the fleets with which you threaten us. Those who defeated you in the early 1980s are still here, along with their sons and grandsons."

We work at the National Counterterrorism Innovation, Technology, and Education (NCITE) Center, a U.S. Department of Homeland Security Center of Excellence based at the University of Nebraska at Omaha. As an interdisciplinary team, our research focuses on emerging threats in the terrorism landscape, often with a pointed focus on the individual leaders at the helm of terrorist organisations and violent extremist movements.

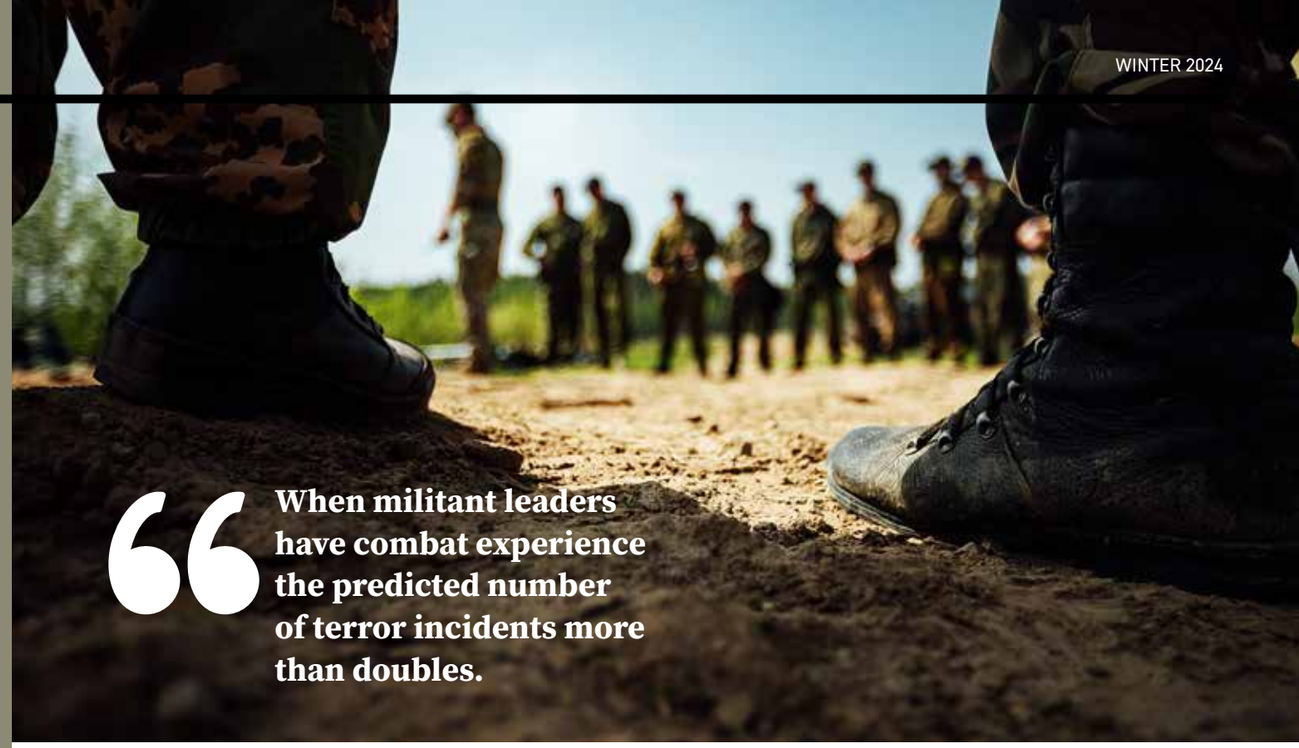
> **More than 95% of terrorism-related fatalities occur in the context of armed conflict.**

It is estimated that more than 95 percent of terrorism-related fatalities occur in the context of armed conflict – perpetrated by local insurgent organisations. According to a recent study, more than 50 percent of insurgent organisations engage in some level of terrorist activity at some point in their campaign. Some militants perpetrate extreme and systemic levels of terrorist violence (e.g., ISIS and the Tamil Tigers), some do so occasionally (e.g., Ansaru and Hayat Tahrir al-Sham), and others conduct little to no terror operations (e.g., the Northern Alliance). These differences matter. Such outcomes are not random as they reflect the decisions, capabilities, and actions of militant actors. Leaders of militant organizations, such as Hassan Nasrallah, Jonas Savimbi, Abu Bakr al-Baghdadi, and Antonio García, are drivers of core militant group actions and potential for action. These individuals are hardly carbon copies of each other, however, each possessing varying capacities as leaders. More formally, it is reasonable to expect that individual-level differences in militant leadership may translate to observable differences in terrorist activity.

Pursuing this hunch, in a study recently published in *Terrorism and Political Violence*, we investigated the relationship between variation in militant leadership and the severity of wartime terrorist violence. Studies from multiple academic fields offer sizable evidence that a leader's set of background experiences shape both how they lead and, more central to our discussion here, how their patterns of decision making translate to organisational outputs.

We build on this body of work to argue that prior experiences play an especially powerful role when militant leaders are selecting between strategies of violence, including terrorism Specifically, to predict group-level differences in this outcome, we emphasise that prior military experiences will shape leaders' willingness to engage in terrorist violence. But military experiences are not necessarily created equal. Rather, we expect differences in militant terrorist activity based on the following mechanisms:

- ***Formal military experiences*** such as those associated with **military training** serve as a restricting influence on terrorist violence; and
- ***Less formal military experiences*** such as **time in active combat** reinforces a mental model for violence as a solution to challenges, increasing the tendency to rely on terrorist violence to achieve desired outcomes.



> **When militant leaders have combat experience the predicted number of terror incidents more than doubles.**

Using new data on the individual backgrounds of militant leaders active between 1989 and 2013, we find support for our expectations. The conditional distribution of the main variables in our sample – leader military experience and terrorism severity – indicates that groups led by individuals with military experience are associated with a higher number of terror attacks in a given year, as well as more terrorism-related fatalities Specifically, relative to those led by individuals *without* military experience, these militant groups conduct an average of roughly 2 more attacks per year with roughly 19 more non-combatants killed in those terrorist attacks, on average, annually.

	Terror Frequency	Terror Lethality
	Group-Year Mean	*Group-Year Mean*
Leader Military Experience: **No**	3,283	10,223
Leader Military Experience: **Yes**	5,248	29,743

Table 1. Conditional Distribution of Main Variables, 1989 – 2013. Source: Doctor, A. C., Hunter, S. T. & Ligon, G. S. (2023).

Looking closer, we find support for our key underlying mechanisms. Based on a set of statistical regression models, we compute the predicted counts of terrorism attacks and terrorism-related fatalities at the group year level based on changes in the leader military experience indicators. We find that when militant leaders have combat experience the predicted number of terror incidents more than doubles and the predicted number of terrorism-related fatalities more than triples in a given year. In contrast, militant groups led by leaders with prior military training are associated with a predicted decrease in lethality.

WHAT DOES THIS MEAN FOR THEORY AND PRACTICE?

Although more research is needed, we identify some key preliminary implications:

- Identifying militant leaders and their background experiences can be a useful and efficient point of leverage for establishing expectations about a fledgling militant group's prospective operational capacity and their future forms of engagement with local communities. For warfighters, analysts, and other practitioners, this can be useful when assessing a threat and proactively allocating resources.
- Leaders can wield independent effects on the contours of terrorist violence, demonstrating that this outcome is a dual function of both structure and agency. To develop actionable recommendations, explanations of terrorism should be able to account for decision making within a range of strategic opportunities and constraints.
- More research is needed on the effects that other experience types may have on militant leader decision making and, relatedly, the performance and behavior of their followers.

Austin C. Doctor is a political scientist at the University of Nebraska at Omaha and the Head of Counterterrorism Research Initiatives at the National Counterterrorism Innovation, Technology, and Education (NCITE) Center. Gina S. Ligon is a professor of collaboration science in the College of Business and the director of NCITE. Sam T. Hunter is a professor of Industrial and Organizational Psychology at the University of Nebraska Omaha and head of strategic initiatives at NCITE.

RACHEL MONAGHAN & BIANCA SLOCOMBE

THE PROSECUTION LANDSCAPE FOR EXTREMIST ACTORS IN THE UK

While the official data can inform us of the number of persons charged, prosecuted and convicted, there is a general absence of detail on this topic. Our research sought to address this.

The United Kingdom (UK) is made up of three distinct legal jurisdictions (i.e., England and Wales, Scotland, and Northern Ireland) with differences in the types of data collected and counting practices with respect to the charging, prosecution and sentencing outcomes (prosecution landscape) of extremist actors. Having said this, the data that is publicly available is merely summary statistics and there is also no separate data available for Scotland. This has subsequently limited the capacity of researchers to analyse overall trends and compare jurisdictional data. Thus, the current study sought to provide a better understanding of the prosecution landscape for extremist actors in the UK by describing, analysing, and comparing the sentencing outcomes of individuals convicted of terrorism, terrorism-related and violent extremism offences over a 21-year time period (April 2001 - March 2022). To this end, we reviewed the relevant literature, undertook interviews with stakeholders, examined a sample of judges' sentencing remarks, and created and analysed a sentencing database to answer a number of key research questions:

Offence Types

Terrorism offences are those offences under terrorism legislation but excluding those offences considered violent extremism. Terrorism-related offences are those offences under other legislation or the common law but which are considered terrorist-related. Violent extremism offences are those offences which "foment, justify or glorify terrorist violence in furtherance of particular beliefs; seek to provoke others to terrorist acts; foment other serious criminal activity or seek to provoke others to serious criminal acts; or foster hatred which might lead to inter-community violence in the UK"

(Crown Prosecution Service, 2015).

1. WHAT CRIMINAL OFFENCES ARE EXTREMIST ACTORS BEING CONVICTED OF?

In our statistical model predicting offence type, Northern Ireland-related extremist actors are far more likely to be convicted of terrorism-related offences than terrorism or violent extremism offences. This is one of the clearest differences evident from the data. Despite being convicted of terrorism and violent extremism in approximately equal proportions, right-wing offenders are the most likely of all motivation groups to be convicted of violent extremism offences, and Islamist offenders are more likely to be convicted of terrorism offences. In England and Wales, the two most frequent principal offences that extremist actors were convicted of were terrorism offences, specifically preparation of acts of terrorism (23%) and collecting information likely to be of use to a person committing or preparing an act of terrorism (14%). In Northern Ireland, the two most frequent principal offences were terrorism-related offences, namely attempting to cause an explosion, or making or keeping explosives with intent to endanger life or property (21%), and the offences of murder, manslaughter and attempted murder (14%). Due to a very small number of cases in Scotland, five principal offences all had the same frequency (14%). Three of these offences constituted terrorism offences.

2. WHAT SENTENCES ARE EXTREMIST ACTORS RECEIVING UPON CONVICTION?

In all jurisdictions, judges and magistrates consider a number of factors when deciding the appropriate sentence for an offender. These factors include the seriousness of the offence, the maximum and minimum penalties contained in the legislation, the range of available disposals (e.g., fines, community sentences or imprisonment), the offender's circumstances, the impact upon the victim, the protection of the public and the existence of mitigating (e.g., age, lack of criminal record, or guilty plea) and aggravating (e.g., lack of remorse, recidivism, and the harm to the victim) factors. Judges and magistrates can also draw upon case law, guideline judgements issued by the Court of Appeal, and where applicable, relevant sentencing guidelines.

Using some of these factors, we found sentence length is influenced by offence type, plea, and total counts (all variables

with legitimate impacts), but sentence length is also impacted by extraneous factors of gender and co-accused (i.e., whether an offender has co-defendants). According to our regression model, an individual most likely to receive the longest sentence would be a male with co-defendants, who does not plead guilty, is accused of multiple counts, and is charged with a terrorism-related offence. In terms of gender, we find that the sentence length for males is nearly two-thirds higher than for females, accounting for other variables. This is consistent with previous research in the US on female terrorist offenders. We did not find evidence that age, jurisdiction, or ethnicity (white vs. non-white) impacted sentence, nor that particular motivation groups received longer sentences than other motivation groups. However, key findings do not account for severity of offences. See the full report for further investigation of severity.

> **...an individual most likely to receive the longest sentence would be a male with co-defendants, who does not plead guilty, is accused of multiple counts, and is charged with a terrorism-related offence.**

3. IS THERE ANY EVIDENCE OF CHANGES IN SENTENCING OVER TIME?

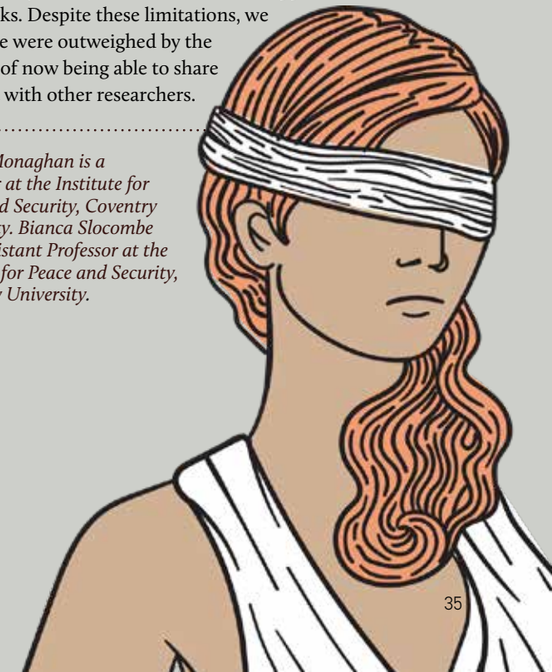
In terms of fluctuations due to changing contextual environments, we were interested in whether sentences increased or decreased in the aftermath of notable terrorism events such as the 7/7 bombings in 2005 and the murder of Jo Cox MP in 2016. However, analysis of sentencing over time revealed that sentence length has remained relatively steady over the years included in the dataset. While two peaks were identified in 2007-2008 and 2017-2018 with respect to the number of Islamist offenders being convicted there was no corresponding change in sentencing outcomes. Similarly, for right-wing offenders the number of individuals convicted peaks in 2018 but there was no corresponding change in sentencing outcomes. These results indicate that significant terrorism events may impact the number of similarly motivated cases sentenced in subsequent years, but do not appear to impact sentence length. This aligns with previous research in the US which found in the periods after the Oklahoma City bombing and 9/11 that the number of individuals indicted increased.

Analysis of all cases in England and Wales reveals no overall difference in sentences after implementation of the 2018 guidelines for terrorism offences, but an overall comparison was limited. Analysis of three specific offences (with adequate samples sizes pre- and post-guidelines) demonstrated an impact of guidelines. The findings demonstrated significant increases, with sentences for preparation of acts of terrorism and dissemination of terrorist publications being ~50%-59% higher (respectively) in the post-guideline period, and collecting information likely to be of use to a person committing or preparing an act of terrorism sentences 85% higher. This is in line with insights from our interviews and wider criminological literature, which suggests that the introduction of sentencing guidelines may have contributed to greater sentence severity.

LIMITATIONS

While our findings provide important insight into the prosecution landscape of extremist actors in the UK, some important limitations must be noted. In examining the prosecution landscape, we do so only by examining those extremist actors who have been convicted and sentenced, and their information is publically available. We are aware that relying on publically available information as an approach has its own drawbacks. Despite these limitations, we feel these were outweighed by the benefits of now being able to share our data with other researchers.

Rachel Monaghan is a Professor at the Institute for Peace and Security, Coventry University. Bianca Slocombe is an Assistant Professor at the Institute for Peace and Security, Coventry University.



JOEL BUSHER, SARAH MARSDEN & LEENA MALKKI

RADICALISATION AND COUNTER-RADICALISATION RESEARCH: PAST, PRESENT AND FUTURE

Research on radicalisation has come on apace over the last two decades. A major new Handbook on Radicalisation and Countering Radicalisation maps its past, present, and future and finds a field in rude health.

INTRODUCTION

From modest beginnings, research on radicalisation and counter-radicalisation now spans disciplinary and theoretical traditions, and informs an international policy agenda concerned with countering and preventing violent extremism (P/CVE). The work that has evolved around the concept of radicalisation has at times been the focus of fierce criticism and debate, but the concept has undoubtedly transformed the way researchers, policymakers and practitioners think about the causes of terrorism and non-state actor political violence. As the 34 chapters that make up the Routledge Handbook on Radicalisation and Countering Radicalisation reveal, in recent years there have been a number of important conceptual, empirical and practical advances in this vibrant field of research.

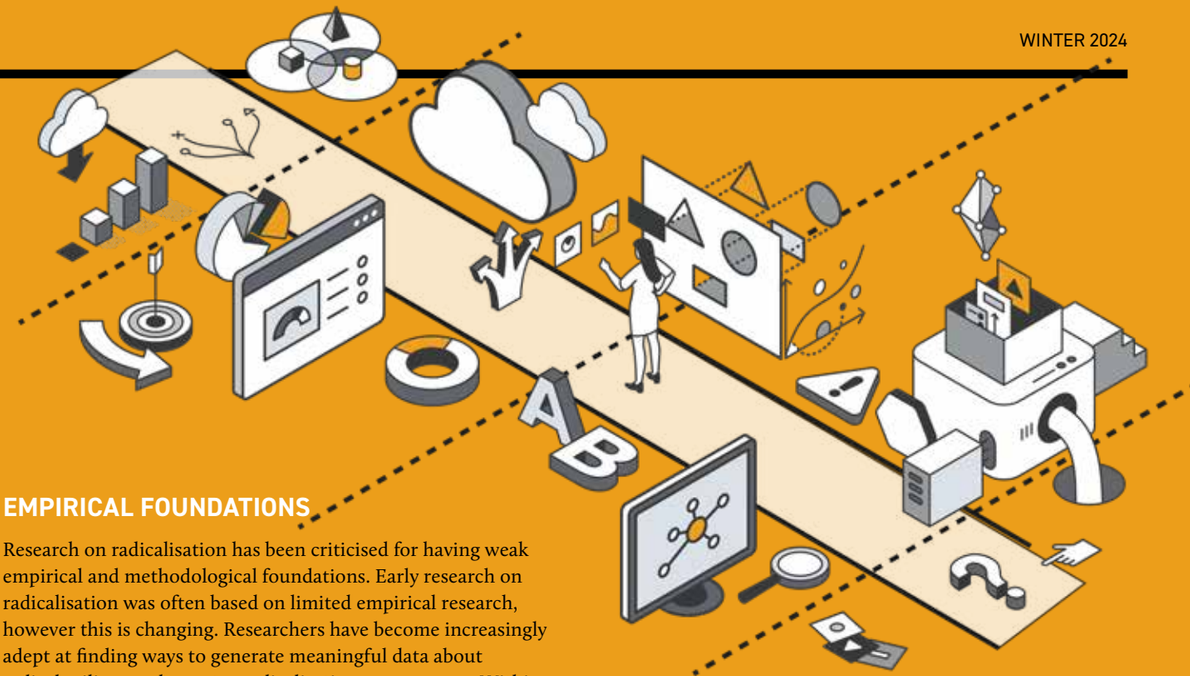
CONCEPTUALISING RADICALISATION

While the concept of radicalisation has sometimes been criticised for being unclear, under-theorised or inconsistent, the flexibility of the concept has arguably been a strength, enabling it to be deployed across diverse scales and geographies. Early criticism of radicalisation research has driven efforts to advance theoretical understanding of radicalisation, from more 'orthodox' and 'critical' perspectives. There are a number of key conceptual take-aways from this research:

- Radicalisation is a process that can and should be studied at different scales. From individual level processes concerned with how and why people adopt radical views or behaviours, to collective processes of group radicalisation, and mass radicalisation, seeking to explain how publics radicalise in contexts of inter-group conflict.
- Models and metaphors for radicalisation have become more sophisticated. Early models and metaphors of staircases and conveyor belts have given way to ones that capture better the dynamic and non-linear nature of radicalisation.

> **Despite the difficulties associated with researching radical milieus, research designs are becoming more sophisticated and access to data is improving.**

- Research is pushing beyond simplistic binaries between cognitive and behavioural radicalisation. Having been a mainstay of early research on radicalisation, contemporary research is seeking to conceptualise the relationship between ideas and behaviours in ways that describe more effectively the complexity of these relationships.
- Radicalisation's relationship to terrorism and violent extremism has been problematised by work that highlights that very few of those who adopt radical ideas or behaviours go on to engage in terrorism.
- Intersectional approaches to radicalisation are starting to emerge, although much more work is needed to understand how interactions between gender, ethnicity, religion and class shape radicalisation processes across different settings.



EMPIRICAL FOUNDATIONS

Research on radicalisation has been criticised for having weak empirical and methodological foundations. Early research on radicalisation was often based on limited empirical research, however this is changing. Researchers have become increasingly adept at finding ways to generate meaningful data about radical milieus and counter-radicalisation programmes. Within the field today there is widespread use of standard social and political science approaches, such as interview-based methods, ethnographic research and surveys, and online research. Nonetheless, limitations and challenges remain:

- Notwithstanding recent interest in the extreme-right, Islamist radicalisation still tends to be the primary ideological focus of radicalisation research, with the literature also dominated by research in the Global North, and focused overwhelmingly on the present. More research is required across under-researched geographic, linguistic, temporal and ideological cases, both to address basic knowledge gaps and to inform theory building and testing.
- Researchers are increasingly leveraging comparative approaches to further understanding of radicalisation and countering radicalisation, such as developing insights into why the vast majority of people with similar backgrounds and experiences to those who engage in violence don't do the same. Nonetheless, such comparative approaches raise significant challenges and questions around how to construct meaningful comparison and what constitutes a credible basis for the shared group-ness of those who do and do not engage in violence.
- There have been some significant advances in the evaluation of P/CVE programmes, but there is an urgent requirement for more research that documents P/CVE programmes and assesses their effects. There is a particular requirement for work on the experience and effects of participation in these programmes.
- As researchers continue to strengthen the evidence base on radicalisation and countering radicalisation, a major challenge will lie in keeping pace with and adapting to the impact of geopolitical shifts, increased societal polarisation, and the rapidly changing technological landscape.

RADICALISATION RESEARCH IN PRACTICE

The chapters in the volume also highlight the extent and vibrancy of debates around the most appropriate ways to carry out research on radicalisation. Ethics are often at the heart of these debates. These include practical issues associated with engaging directly with those involved in radical spaces and the risks it poses to participants and researchers. Direct engagement with policy planners and practitioners also generates ethical issues around the influence of policy planner/practitioner priorities on research agendas and practice.

The need to safeguard researcher safety and well-being is also beginning to receive welcome and overdue attention.

CONCLUSION

The research set out in the Handbook demonstrates that although there is much more to be done, understanding of radicalisation and counter-radicalisation has advanced significantly since the early 2000s.

Joel Busher is Professor of Political Sociology at the Centre for Trust, Peace and Social Relations, Coventry University.

Sarah Marsden is Director of the Handa Centre for the Study of Terrorism and Political Violence at the University of St Andrews.

Leena Malkki is Director of the Centre for European Studies at the University of Helsinki.

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/communication*

JOEL BUSHER, SARAH MARSDEN & LEENA MALKKI: RADICALISATION AND COUNTER-RADICALISATION RESEARCH: PAST, PRESENT AND FUTURE

Baker-Beall, C., Heath-Kelly, C., & Jarvis, L. (2015). Counter-radicalisation in Europe: Critical perspectives. Routledge.

Busher, J., L. Malkki, and Marsden, S.V. (2023). The Routledge Handbook on Radicalisation and Countering Radicalisation. Routledge.

Morrison, J. F., Silke, A., & Bont, E. (2021). The development of the framework for research ethics in terrorism studies (FRETS). *Terrorism and Political Violence*, 33 (2), 271–289. *http://tinyurl.com/5d9tusce*

Phillips, B. J. (2023). How did 9/11 affect terrorism research? Examining articles and authors, 1970–2019. *Terrorism and Political Violence*, 35 (2), 409–432. *http://tinyurl.com/4c88huza*

Richards, A. (2015). From terrorism to 'radicalization' to 'extremism': Counterterrorism imperative or loss of focus? *International Affairs*, 91 (2), 371–380. *http://tinyurl.com/4ft2chvp*

Schuurman, B. (2020). Research on terrorism, 2007–2016: A review of data, methods, and authorship. *Terrorism and Political Violence*, 32 (5), 1011–1026. *http://tinyurl.com/7b7ptufe*

VINCENT DENAULT & ALDERT VRIJ: "THE EYES CAN'T LIE": MISCONCEPTIONS ABOUT NONVERBAL COMMUNICATION AND WHY THEY MATTER

Denault, V., & Zloteanu, M. (2022). Darwin's illegitimate children: how body language experts undermine Darwin's legacy. *Evolutionary Human Sciences*. *http://tinyurl.com/mr36v4f2*

Denault, V., Plusquellec, P., Jupe, L. M., *et al.* (2020). The analysis of nonverbal communication: The dangers of pseudoscience in security and justice contexts. *Anuario de Psicología Jurídica*, 30, 1-12. *http://tinyurl.com/3wy6ru4r*

Hall, J. A., Horgan, T. G., & Murphy, N. A. (2019). Nonverbal communication. *Annual Review of Psychology*, 70, 271–294. *http://tinyurl.com/yjty9ysy*

Mann, S., Deeb, H., Vrij, A., Hope, L., & Pontigia, L. (2020). Detecting smugglers: identifying strategies and behaviors in individuals in possession of illicit objects. *Applied Cognitive Psychology*, 34, 372–386. *http://tinyurl.com/4furvmy3*

Mann, S., Vrij, A., Nasholm, E., Warmelink, L., Leal, S., & Forrester, D. (2012). The direction of deception: Neuro-Linguistic Programming as a lie detection tool. *Journal of Police and Criminal Psychology*, 27, 160-166. *http://tinyurl.com/4mn6bjy7*

Patterson, M. L., Fridlund, A. J., & Crivelli, C. (2023). Four misconceptions about nonverbal communication. *Perspectives on Psychological Science*. *http://tinyurl.com/372vwjbc*

Plusquellec, P., & Denault, V. (2018). The 1000 most cited papers on visible nonverbal behavior: A bibliometric analysis. *Journal of Nonverbal Behavior*, 42(3), 347-377. *http://tinyurl.com/3syw7rd6*

Sweet, D. M., Meissner C. A., & Atkinson D. J. (2017). Assessing law enforcement performance in behavior-based threat detection tasks involving a concealed weapon or device. *Law and Human Behavior*, 41, 411-421.

National Protective Security Authority (2023). Behavioural Detection. Retrieved from *http://tinyurl.com/2384ab2p*

Vrij, A., Hartwig, M., & Granhag, P.A. (2019). Reading lies: Nonverbal communication and deception. *Annual Review of Psychology*, 70(1), 295–317. *http://tinyurl.com/cxr5thh3*

AUSTIN DOCTOR, GINA LIGON & SAM HUNTER: MILITANT LEADERSHIP AND THE SEVERITY OF TERRORISM IN CONFLICT ENVIRONMENTS

Doctor A. C., Hunter, S. H., & Ligon, G. L. (2023). Militant Leadership and Terrorism in Armed Conflict, *Terrorism and Political Violence*. *http://tinyurl.com/3pfbvxze*

Polo, S. M. T., & González, B. (2020). The Power to Resist: Mobilization and the Logic of Terrorist Attacks in Civil War. *Comparative Political Studies*, 53(13), 2029-2060. *http://tinyurl.com/44abmvk*

National Counterterrorism Innovation, Technology, and Education Center (NCITE) available at: *http://tinyurl.com/3bp82jpd*

The Global Terrorism Index (GTI) available at: *http://tinyurl.com/ycxvmeb2*

LINA HILLNER: UNEXPLORED INTERACTIONS: DISENTANGLING TRUSTWORTHINESS, TRUST AND RAPPORT

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of management review*, 20(3), 709-734. *http://tinyurl.com/4pdaase8*

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: A meta-analytic test of their unique relationships with risk taking and job performance. *Journal of Applied Psychology*, 92(4), 909–927. *http://tinyurl.com/wa9b7xsb*

Oleszkiewicz, S., Atkinson, D. J., Kleinman, S., & Meissner, C. A. (2023). Building Trust to Enhance Elicitation. *International Journal of Intelligence and CounterIntelligence*, 1-22. *http://tinyurl.com/452w8xba*

Neequaye, D. A., & Mac Giolla, E. (2022). The use of the term rapport in the investigative interviewing literature: A critical examination of definitions. *Meta-Psychology*, 6. *http://tinyurl.com/yeyu63c3*

Tickle-Degnen, L., & Rosenthal, R. (1990). The nature of rapport and its nonverbal correlates. *Psychological inquiry*, 1(4), 285-293. *http://tinyurl.com/mu4s247u*

Alison, L., Alison, E., Noone, G., Elntib, S., Waring, S., & Christiansen, P. (2014). The efficacy of rapport-based techniques for minimizing counter-interrogation tactics amongst a field sample of terrorists. *Psychology, Public Policy, and Law*, 20(4), 421–430. *http://tinyurl.com/3wy4fctr*

Dianiska, R. E., Swanner, J. K., Brimbal, L., & Meissner, C. A. (2021). Using disclosure, common ground, and verification to build rapport and elicit information. *Psychology, Public Policy, and Law*, 27(3), 341–353. *http://tinyurl.com/4nxjuftd*

Hillner, L., Hope, L., Kontogianni, F., & Conchie, S. (2023). *The role of trustworthiness and rapport in computer-mediated information elicitation* [Conference session]. Behavioural and Social Science in Security (BASS23) conference. Bath, United Kingdom.

LORRAINE HOPE: NAVIGATING THE CROSS-CULTURAL CHALLENGES FOR EFFECTIVE RAPPORT AND INFORMATION GATHERING

Hope, L., Anakwah, N., Antfolk, J., Brubacher, S.P., Flowe, H., Gabbert, F., Giebels, E., Kanja, W., Korkman, J., Kyo, A., Naka, M., Otgaar, H., Powell, M. B., Selim, H., Skrifvars, J., Sorkpah, I. K., Sowatey, E. A., Steele, L. C., Wells, S., ... Anonymous (2022). Urgent issues and prospects at the intersection of culture, memory, and witness interviews: Exploring the challenges for research and practice. *Legal and Criminological Psychology*, 27, 1–31. *http://tinyurl.com/y5w7k24z*

Anakwah, N., Horselenberg, R., Hope, L., Amankwah-Poku, M., & van Koppen, P. J. (2020). Cross-cultural differences in eyewitness memory reports. *Applied Cognitive Psychology*, 34, 504–515. *http://tinyurl.com/3zjxycce*

Wang, Q. (2021). The Cultural Foundation of Human Memory, *Annual Review of Psychology*, 72, 151-179. *http://tinyurl.com/39mttxkr*

ANASTASIA KORDONI, SHENGNAN LIU, MIRIAM KOSCHATE-REIS & MARK LEVINE: INVESTIGATING THE INFLUENCE OF HYBRID SOCIAL IDENTITIES IN ONLINE COMMUNITIES

Farrell-Molloy, J., & Macklin, G. (2022). Ted Kaczynski, Anti-Technology Radicalism and Eco-Fascism. *http://tinyurl.com/4zf94bcc*

Hernández-Campoy, J. M. (2016). Sociolinguistic styles. Wiley-Blackwell.

Koschate, M., Naserian, E., Dickens, L., Stuart, A., Russo, A., & Levine, M. (2021). ASIA: Automated Social Identity Assessment using linguistic style. *Behavior Research Methods*, 1-20. *http://tinyurl.com/2c92c35h*

Spears, R. (2021). Social influence and group identity. *Annual Review of Psychology*, 72, 367-390. *http://tinyurl.com/4ywcvf4h*

MARC KYDD, LYNSAY SHEPHERD, GRAHAM JOHNSON & ANDREA SZYMKOWIAK: LOVE BYTES – IMPROVING ROMANCE FRAUD PREVENTION

I.C.C.C. (2013). 2013 IC3 Annual Report. Available at: *http://tinyurl.com/nbtksa6u*

I.C.C.C. (2023). 2022 IC3 Annual Report. Available at: *http://tinyurl.com/vfd6mdca*

Cross, C. and Kelly, M. (2016). The problem of 'white noise': examining current prevention approaches to online fraud, *Journal of Financial Crime*, Vol. 23 No. 4, pp. 806-818. *http://tinyurl.com/3fbv3zxs*

Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., & Ebner, N. C. (2019). Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. ACM transactions on computer-human interaction: a publication of the Association for Computing Machinery, 26(5), 32. *http://tinyurl.com/5y9fhmyf*

Cross, C., & Layt, R. (2022). I Suspect That the Pictures Are Stolen: Romance Fraud, Identity Crime, and Responding to Suspicions of Inauthentic Identities. *Social Science Computer Review*, 40(4), 955–973. *http://tinyurl.com/4wfmakyy*

Maeng, W., & Lee, J. (2022). *Designing and Evaluating a Chatbot for Survivors of Image-Based Sexual Abuse*. Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems.

Cassandra Cross (2019). You're not alone: the use of peer support groups for fraud victims, *Journal of Human Behavior in the Social Environment*, 29:5, 672-691. *http://tinyurl.com/2accmsfb*

Van Uden-Kraan, C. F., Drossaert, C. H., Taal, E., Smit, W. M., Bernelot Moens, H. J., & Van de Laar, M. A. (2011). Determinants of engagement in face-to-face and online patient support groups. *Journal of medical Internet research*, 13(4), e106. *http://tinyurl.com/bdcs3p2e*

Correia, S.G. (2019). Responding to victimisation in a digital world: a case study of fraud and computer misuse reported in Wales. *Crime Science*, 8, 4. *http://tinyurl.com/59cw2zuu*

Norris, G., Brookes, A. & Dowell, D. (2019). The Psychology of Internet Fraud Victimisation: a Systematic Review. *Journal of Police and Criminal Psychology*, 34, 231–245. *http://tinyurl.com/2p8xanwd*

RACHEL MONAGHAN & BIANCA SLOCOMBE: THE PROSECUTION LANDSCAPE FOR EXTREMIST ACTORS IN THE UK

Alexander, A. and Turkington, R. (2018). Treatment of terrorists: How does gender affect justice? *CTC Sentinel*, 11(8), 24-29. *http://tinyurl.com/bdz482tx*

Allen, R. (2016). The Sentencing Council for England and Wales: Brake or Accelerator on the Use of Prison? *Transform Justice.* http://tinyurl.com/bmnz43d8

Allen, G., Burton, M., Pratt, A. (2022). Terrorism in Great Britain: the statistics. Commons Library Research Briefing. London: House of Commons Library. http://tinyurl.com/bdwy43tr

Amirault, J., Bouchard, M. (2017). Timing is everything: The role of contextual and terrorism-specific factors in the sentencing outcomes of terrorist offenders. *European Journal of Criminology*, 14(3), 269-289.

Blackbourn, J. (2021). Counterterrorism legislation and far-right terrorism in Australia and the United Kingdom. *Common Law World Review*, 50(1), 76-92. http://tinyurl.com/67hrrd3b

Crown Prosecution Service (2015). Violent Extremism and Related Criminal Offences. http://tinyurl.com/4ht22r6f

Damphousse, K.R., Shields, C. (2007). The morning after: Assessing the effect of major terrorism events on prosecution strategies and outcomes. *Journal of Contemporary Criminal Justice*, 23(2), 174-194. http://tinyurl.com/435ydpv5

Gill, P. (2020). The data collection challenge: Experiences studying lone-actor terrorism. Washington, D.C.: RESOLVE Network. http://tinyurl.com/3ajmf7x2

Jupp, J. (2022). From Spiral to Stasis? United Kingdom counter-terrorism legislation and extreme right-wing terrorism. *Studies in Conflict & Terrorism*. http://tinyurl.com/57muhhwp

DAVID A. NEEQUAYE: HOW PEOPLE DECIDE WHAT TO DISCLOSE IN INVESTIGATIVE INTERVIEWS

Granhag, P. A., Montecinos, S. C., & Oleszkiewicz, S. (2015). Eliciting intelligence from sources: The first scientific test of the Scharff technique. *Legal and Criminological Psychology*, 20(1), 96–113. http://tinyurl.com/mpjh8ucn

Neequaye, D. A., Granhag, P. A., & Luke, T. J. (2023). Exploring how members of illicit networks navigate investigative interviews. *Royal Society Open Science*, 10(5), 230450. http://tinyurl.com/yxea2vm7

Neequaye, D. A., Luke, T. J., & Kollback, K. (2021). Managing Disclosure Outcomes in Intelligence Interviews. *PsyArXiv*. http://tinyurl.com/yd4a4hus

Soufan, A. (2011). The Black Banners: The Inside Story of 9/11 and the War Against al-Qaeda. W. W. Norton & Company.

BECKY PHYTHIAN: LAW ENFORCEMENT INFORMATION SHARING FOR THE 21ST CENTURY

Brown, R. (2018). Understanding law enforcement information sharing for criminal intelligence purposes (No. 566). *Australian Institute of Criminology Trends and Issues in Crime and Criminal Justice*. http://tinyurl.com/2fx57ykp

Caparini, M. (2022). *Transnational organized crime: A threat to global public goods*. Stockholm International Peace Research Institute. http://tinyurl.com/4ma58tju

Kirby, S., & Keay, S. (2021). Improving Intelligence Analysis in Policing. Routledge.

Phythian, R., & Kirby, S. (2022). What does the UK Police National Database tell us about the future of police intelligence? *Policing: A Journal of Policy and Practice*, 17, 1-14. http://tinyurl.com/444n4z84

Phythian, R., Kirby, S., & Swan-Keig, L. (2024). Understanding how law enforcement agencies share information in an intelligence-led environment: how operational context influences different approaches. P*olicing: An International Journal*. http://tinyurl.com/yc4nfj7y

Stock, J. (2023). There is an epidemic of transnational crime. We need a global response. The Guardian. http://tinyurl.com/24xydtst

DANA ROEMLING & JACK GRIEVE: FORENSIC AUTHORSHIP ANALYSIS

Coulthard, M., Johnson, A., & Wright, D. (2016). An Introduction to Forensic Linguistics: Language in Evidence (2nd Ed). Routledge. http://tinyurl.com/4a62d7jd

Grant, T., & Grieve, J. (2022). The Starbuck case: Methods for addressing confirmation bias in forensic authorship analysis. In I. Picornell, R. Perkins, & M. Coulthard (Eds.), *Methodologies and Challenges in Forensic Linguistic Casework* (First Edition, pp. 13–28). Wiley Blackwell. http://tinyurl.com/mru4f4nr

Nini, A. (2018). Developing forensic authorship profiling. *Language and Law / Linguagem e Direito*, 5(2), 38–58. http://tinyurl.com/2yrywfev

Nini, A. (2023). A Theory of Linguistic Individuality for Authorship Analysis (1st ed.). Cambridge University Press. http://tinyurl.com/2rk7nfzf

Shuy, R. W. (2001). DARE's role in linguistic profiling. *Dictionary of American Regional English Newsletter,* 4(3), Article 3. http://tinyurl.com/4ypfd8ew

Svartvik, J. (1968). The Evans statements: A case for forensic linguistics. University of Goteborg. http://tinyurl.com/bdzja6yh

NADINE SALMAN & ZAINAB AL-ATTAR: NEURODIVERGENCE AND EXTREMISM: CONSIDERATIONS FOR PRACTICE

Al-Attar, Z. (2018). Interviewing Terrorism Suspects and Offenders with an Autism Spectrum Disorder. *The International Journal of Forensic Mental Health*, 17(4), 321–337. http://tinyurl.com/4tvn35dn

Al-Attar, Z. (2019). Extremism, radicalisation & mental health: Handbook for practitioners. Radicalisation Awareness Network: Health & Social Care Subgroup, *European Commission*. http://tinyurl.com/3f66k8wn

Al-Attar, Z. (2020). Autism spectrum disorders and terrorism: How different features of autism can contextualise vulnerability and resilience. *Journal of Forensic Psychiatry and Psychology*, 31(6), 926–949. http://tinyurl.com/yeve373y

Salman, N. L., Al-Attar, Z. (2023). A Systematic Review of Neurodivergence, Vulnerability, and Risk in the Context of Violent Extremism. http://tinyurl.com/mjtsvr7a

Salman, N. L., Al-Attar, Z., Mckenzie, G. (2023). Practitioner Perspectives on Counterterrorism and Neurodiversity. http://tinyurl.com/4y2ncwu2

Salman, N. L., Al-Attar, Z., Pyszora, N., Smith, D., Iqbal, M. (2023). Neurodivergence and Violent Extremism: 18 International Case Studies. http://tinyurl.com/4bnkcc55

Worthington, R., Al-Attar, Z., Lewis, A., & Pyszora, N. (2021). Rapid Evidence Assessment (REA) on Neurodiversity and Violent Extremism. AVERT. http://tinyurl.com/yuystp3x

MATTIAS SJÖBERG: INTERPERSONAL SENSEMAKING: A POWERFUL TOOL FOR FACILITATING COOPERATION IN SUSPECTS

Sjöberg, M., Taylor, P. J., Conchie, S. M. (2023). The cylinder model. In G. Oxburgh et al. (Eds.), Interviewing and interrogation: A review of research and practice since World War II. *Florence, Torkel Opsahl Academic EPublisher*. http://tinyurl.com/5dp7mwse

Taylor, P. J. (2002). A cylindrical model of communication behavior in crisis negotiations. *Human Communication Research*, 28(1), 7-48. http://tinyurl.com/t65mpkyn

Taylor, P. J. (2014). The role of language in conflict and conflict resolution. In T. M. Holtgraves (Ed.), *The oxford handbook of language and social psychology* (pp. 459-470). Oxford: Oxford University Press. http://tinyurl.com/za9sprbw

Wells, S., & Brandon, S. E. (2019). Interviewing in criminal and intelligence-gathering contexts: Applying science. *International Journal of Forensic Mental Health*, 18(1), 50-65. http://tinyurl.com/yczckbte

LAURA G. E. SMITH: DIGITAL TRACES OF OFFLINE MOBILISATION

Brown, O., Lowery, C., & Smith, L. G. E. (2022). How opposing ideological groups use online interactions to justify and mobilise collective action. *European Journal of Social Psychology*, 52, 1082–1110. http://tinyurl.com/ybmwr2hb

Hinds, J., Brown, O., Smith, L. G. E., Piwek, L., Ellis, D. A., & Joinson, A. N. (2022). Integrating Insights About Human Movement Patterns From Digital Data Into Psychological Science. *Current Directions in Psychological Science*, 31(1), 88-95. http://tinyurl.com/ytvwj7u2

Smith, L. G. E., Blackwood, L., & Thomas, E. F. (2020). The Need to Refocus on the Group as the Site of Radicalization. *Perspectives on Psychological Science*, 15(2), 327-352. http://tinyurl.com/3tspc7a9

Smith, L. G. E., Piwek, L., Hinds, J., Brown, O., & Joinson, A. (2023). Digital traces of offline mobilization. *Journal of Personality and Social Psychology*, 125(3), 496–518. http://tinyurl.com/44eu6hp2

Smith, L. G. E., Thomas, E. F., & McGarty, C. (2015). "We must be the change we want to see in the world": integrating norms and identities through social interaction. *Political Psychology*, 36(5), 543-557. http://tinyurl.com/3h3fprsb

Smith, L. G. E., Wakeford, L., Cribbin, T. F., Barnett, J., & Hou, W. K. (2020). Detecting psychological change through mobilizing interactions and changes in extremist linguistic style. *Computers in Human Behavior*, 108, 106298. http://tinyurl.com/yeyw83ew

Thomas, E. F., Duncan, L., McGarty, C., Louis, W. R., & Smith, L. G. E. (2022). MOBILISE: A Higher Order Integration of Collective Action Research to Address Global Challenges. *Advances in Political Psychology,* 43(S1), 107-164. http://tinyurl.com/2a39t9m9

LAURA M. STEVENS, TIA BENNETT, SARAH ROCKOWITZ, & HEATHER D. FLOWE: THE ROLE OF DIGITAL TECHNOLOGIES (GBVXTECH) IN COMMUNICATING GENDER-BASED VIOLENCE

Hillis, S., Mercy, J., Amobi, A. & Kress, H. (2016). Global Prevalence of Past-year Violence Against Children: A Systematic Review and Minimum Estimates. *Pediatrics*; 137 (3). http://tinyurl.com/2jwm2mhf

Stevens, L. M., Bennett, T., Cotton, J., Rockowitz, S., & Flowe, H. (2024). A Critical Analysis of Gender-Based Violence Reporting and Evidence Building Applications (GBVxTech) for Capturing Memory Reports. *Frontiers in Psychology*, 14, 1289817. http://tinyurl.com/9sjz7dny

World Health Organization (2002). WHO Multi-Country Study on Women's Health and Domestic Violence Against Women. http://tinyurl.com/mrytz2rf

World Health Organization (2021). Violence against women prevalence estimates, 2018. http://tinyurl.com/2eampy35

NICK VAN DER KLOK, MIRIAM S. D. OOSTINGA, LUKE C. RUSSELL & MICHAEL A. YANSICK: ACCELERATING INFLUENCE: CHALLENGING THE LINEAR PARADIGM OF SUICIDE NEGOTIATION

Ireland, C. A., & Vecchi, G. M. (2009). The Behavioral Influence Stairway Model (BISM): framework for managing terrorist crisis situations? *Behavioral Sciences of Terrorism and Political Aggression*, 1(3), 203–218. http://tinyurl.com/49vj8t6m

Oostinga, M. S. D., Van der Klok, N., Watson, S. J., & Russell, L. C. (in preparation). Timing of Behaviour Change in Crisis Negotiation: A Temporal Test of the Revised Behavioural Influence Stairway Model. http://tinyurl.com/yb5rj5bf

Vecchi, G. M., Van Hasselt, V. B., & Romano, S. J. (2005). Crisis (hostage) negotiation: current strategies and issues in high-risk conflict resolution. *Aggression and Violent Behavior*, 10(5), 533–551. http://tinyurl.com/3tfnmebt

Vecchi, G. M., Wong, G. K., Wong, P. W., & Markey, M. A. (2019). Negotiating in the skies of Hong Kong: The efficacy of the Behavioral Influence Stairway Model (BISM) in suicidal crisis situations. *Aggression and Violent Behavior*, 48, 230–239. http://tinyurl.com/3k4ek3f6

RESOURCES ON COMMUNICATION

Take a look at some of our past CREST guides, reports, and *CREST Security Review* articles around the topic of communication.

ALISON, HUMANN & WARING: COMMUNICATING WITH CASUALTIES IN EMERGENCIES (CSR#6)

Both survivor testimonies and research reveal that there are many ways in which we can react in an emergency

https://crestresearch.ac.uk/comment/communicating-casualties-emergencies/

DANCE: ADDRESSING ALGORITHMS IN DISINFORMATION (CSR#17)

A look at how people discuss false content online and how exploring social media discourses can help strengthen policy responses.

https://crestresearch.ac.uk/comment/addressing-algorithms-in-disinformation/

DOUGLAS ET AL: CONSPIRACY THEORIES: HOW ARE THEY ADOPTED, COMMUNICATED, AND WHAT ARE THEIR RISKS?

This report examines why people adopt conspiracy theories, how they are communicated, and what their risks are.

https://crestresearch.ac.uk/resources/conspiracy-theories-douglas-full-report/

MAHER, AMARASINGAM & WINTER: HOW TELEGRAM DISRUPTION IMPACTS JIHADIST PLATFORM MIGRATION

This report investigates the impact of two Action Days geared towards meaningfully disrupting jihadist networks on Telegram, conducted by Europol in 2018 and 2019.

https://crestresearch.ac.uk/resources/how-telegram-disruption-impacts-jihadist-platform-migration/

OOSTINGA: COMMUNICATION ERROR HANDLING IN SUSPECT INTERVIEWS AND CRISIS NEGOTIATIONS (CSR#6)

In suspect interviews and crisis negotiations we don't always make the correct decisions. How can we recover from different kinds of communication errors?

https://crestresearch.ac.uk/comment/communication-error-handling/

POWER ET AL: THE PSYCHOLOGY OF INTEROPERABILITY: BUILDING BETTER MULTI-AGENCY COUNTER-TERRORISM TRAINING (INTEROP)

This project's outputs review past challenges to interoperability between the UK Emergency Services and identify a framework to systematically identify behavioural and verbal indicators.

https://crestresearch.ac.uk/projects/the-psychology-of-interoperability/

RICE, INNES & RATCLIFFE: STARS: PUBLIC-FACING COUNTER-TERRORISM STRATEGIC COMMUNICATION CAMPAIGNS

This project's outputs explore how and why communication campaigns designed to deter terrorism and deliver influence over public behaviour, achieve differing outcomes.

https://crestresearch.ac.uk/projects/situational-threat-and-response-signals-stars/

ROGERS ET AL: COMMUNICATING EFFECTIVELY WITH THE PUBLIC ABOUT TERRORISM IN CROWDED PLACES (CSR#11)

How effective is public messaging in promoting protective health behaviours and how does this impact the public's perception of and likely response to a terror attack?

https://crestresearch.ac.uk/resources/communicating-effectively-with-the-public-about-terrorism-in-crowded-places/

STEEN: A COMMUNICATION PERSPECTIVE ON RESILIENCE (CSR#16)

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

https://crestresearch.ac.uk/comment/a-communication-perspective-on-resilience/

TAYLOR: COMMUNICATING ACROSS CULTURES (CSR#7)

From small talk to empathising, this article outlines some of the potential pitfalls and gaps in cross-cultural understanding.

https://crestresearch.ac.uk/comment/communicating-across-cultures/

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 220 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 X/Twitter, @crest_research