CSR

COVID-19
Behavioural and social science responses to the pandemic

CONTENTS

Highlights

THE GROUND TRUTH AFTER-ACTION REVIEW TOOL

The after-action review tool Ground TRUTH helps prepare for, adapt to, and recover from critical incidents – p18

. . . .

BALANCING CYBERSECURITY AND PRIVACY IN THE REMOTE WORKFORCE

Remote working will only truly work if we get the balance of security and privacy right – p20

COVID-19

FROM THE EDITOR

The COVID-19 pandemic triggered the biggest global crisis of our time, with lasting changes to society from how we shake hands, where we work, how we hold meetings, travel and socialise, to our perceptions of risk, law and order, and privacy.

As we grasp its continuing impact on society, this issue of *CREST Security Review* highlights some of the responses of behavioural and social science researchers to the pandemic, applying novel lessons to security threats caused or exacerbated by the outbreak.

On the topic of pandemic-led conspiracies, Michele Grossman (page 4) explains how these conspiracies can breed susceptibility to violent extremist thinking and action. Anti-vaccination misinformation has demonstrable adverse consequences, hindering our ability to respond effectively to a crisis, but Stephan Lewandowsky and Muhsin Yesilada give us hope as they discuss inoculation on page 16. And is there a link between a rise of the far right and COVID-19 related conspiracy theories? Lorraine Bowman Grieve (page 22) looks at the evidence in Ireland.

Highlighting challenges during emergencies: Liv Brown (page 14) examines how multi-agency emergency responders communicated and coordinated their tasks; on page 18 Laurence Alison and his team say during fast-moving, high-stakes, and chronic critical incidents, psychological support needs to be rapid, and efficient – that's where their TRUTH after-action review tool comes in; and tasked with supporting the resilience, performance, and health of frontline workers during the initial response to COVID-19, Nathan Smith and Emma Barrett discuss how their rapid response process can be applied to the work of security practitioners facing similarly demanding situations in the future (page 6).

On page 10, Lorraine Hope, Rachel Zajac, and Maryanne Garry explain why contact tracing needs a dose of memory science, while on page 12 Jordan Nunan and Ian Stanier investigate how intelligence gathering adapted to the pandemic, providing key findings from conversations with informant handlers.

Meanwhile, remote working will only truly work if we get the balance of security and privacy right, says Jason Nurse, as he discusses the top four concerns for securing the remote workforce on page 20.

Outside of this issue's focus on the pandemic, Anna Leslie walks us through the Eliciting Information Framework on page 30, designed to assist practitioners in enabling them to apply the research more easily to their work.

Derived from a systematic review of contemporary research, a new model

for understanding disengagement and deradicalisation processes has also been produced. Andrew Silke and colleagues, the team behind the Phoenix Model, take us through its development on page 24.

Finally, understanding and attempting to counter the appeal of extremist media requires appreciation of the techniques used to provide engrossing narratives. Simon Copeland talks Photoshop, filters and the Islamic State on page 28.

You can find all the research that underpins these articles and some further reading in the 'Read More' section on page 34. Please let me know what you liked (or didn't) about this issue and what you would like to see featured in future issues. Write to me at *b.stevens@lancaster.ac.uk*

Rebecca Stevens
Editor, *CSR*

MICHELE GROSSMAN

HOW HAS COVID-19 CHANGED THE VIOLENT EXTREMIST LANDSCAPE?

Coronavirus has highlighted how anxiety, uncertainty, and the reordering of democratic state-citizen relations can breed susceptibility to violent extremist thinking and action.

THE NOT-SO-NEW NEW WORLD ORDER

The COVID-19 pandemic has upended the normative social order of democratic societies in profound ways: lockdowns, public health mandates, a range of restrictions on movement and behaviour, and the rapid development of new-generation vaccines. This disruption has occurred amid an environment of risk and uncertainty that threatens peoples' sense of security, stability, and resilience. The rise of pandemic-led conspiracy thinking has therefore been predictable.

There is a well-established relationship between conspiracy narratives and the sense of threat, particularly concerning system identity threat, or the view that society is fundamentally changing. QAnon influencers, for example, quickly harnessed their conspiracy movement's anti-government, 'Deep State' narrative of corrupt, shadowy elites to fit with how states around the world were responding to the pandemic's public health threats.

However, QAnon's dark prophesies of a New World Order that would upend civilisation is not new, drawing together a pastiche of familiar, pre-existing militant narratives based on anti-Semitism, white nationalism, anti-vaccination, and anti-technology discourse.

Some of these older militant narratives have long been associated with violent action against minorities and violent resistance to the state. It is, therefore, unsurprising that the rise of pandemic-inspired conspiracist movements has been escalated and capitalised on by violent extremist movements across the board.

Europol has warned that COVID-19 will continue to escalate violent extremist threats in various countries, increasing tolerance for violence in response to pandemic-induced stressors. This runs alongside evidence that ideologically diverse violent extremist networks are exploiting pandemic-related vulnerabilities through online propaganda and recruitment efforts.

As our AVERT Research Network submission to Australia's parliamentary inquiry on extremist movements and radicalism argues, the extension of government authority and curtailing of individual liberties during a public health emergency have been consistently reframed by extremists as instruments of social control, government corruption, and state illegitimacy, accelerating what Ehud Sprinzak (1991) terms the 'transformational delegitimation' of democratic societies and institutions.

NEW GATEWAYS TO VIOLENT EXTREMISM

While QAnon influencers were predictably nimble in exploiting gateway online anti-child abuse and exploitation networks to grow their impact, the pandemic-inspired intersection of lifestyle and wellness, violent extremism, and conspiracy networks (Khalil, 2021) has been more novel.

In Australia, the former chef and dietary wellness influencer Pete Evans posted the neo-Nazi 'sonnenrad' or 'black sun' swastika for his many online followers, a symbol appropriated by the Nazis to signal the rebirth of Aryanism. Other wellness influencers have also energetically sought to monetise the surge of interest in anti-authority conspiracies by promoting product-based resistance to public health measures.

THE WEAPONISATION OF COVID-19

The promotion of conspiracies and disinformation can be understood as a form of attack (CRIS, 2021). For those who seek to escalate violent conflict, accelerate civil unrest, and enhance social and political polarisation, COVID-19 has been a swiftly weaponised gift, for example, by encouraging followers to deliberately spread COVID-19 as a means of hastening the collapse of civilisation or the elimination of hated others. These efforts have been significantly aided by the shift to extensive online social interaction as well as information-gathering to make sense of the upheaval.

> "For those who seek to escalate violent conflict, accelerate civil unrest, and enhance social and political polarisation, COVID-19 has been a swiftly weaponised gift"

This is particularly the case for young people who are arguably bearing a disproportionate pandemic-related burden in terms of disrupted schooling, dwindling or precarious employment, isolation from face-to-face culturally diversified social settings, and mental health and housing challenges (Lowe, 2021). Under these circumstances, the vulnerability of young people – already a generation of digital natives – to the online social harms of violent extremist conspiratorial ideologies can intensify.

ADDRESSING THE INTERSECTION OF COVID-19 AND EXTREMIST IDEOLOGIES

A key question raised by the impact of the pandemic on drivers toward violent extremism is whether these impacts are likely to be acute or chronic.

Will the cessation or moderation of the pandemic, driven by increased global vaccination rates and the restoring of individual liberties and movement, see extremist conspiracy uptake subside? Or will the longer-term social, economic, and political impacts of the pandemic, which may well outlast the immediate public health crisis, provide fertile ground for continuing political and social polarisation that extremists can channel toward violent action?

> "Will the cessation or moderation of the pandemic see extremist conspiracy uptake subside? Or will COVID-19's longer-term impacts provide fertile ground that extremists can channel toward violence?"

While we may not be able to answer this question yet, we should be prepared for both scenarios. A key response for policymakers is to recognise and address:

1. The role that conspiratorial thinking plays in processes of radicalisation

2. The emergence of conspiracist movements as critical extremist actors (AVERT, 2021)

3. Whether strategies for inoculating or 'pre-bunking' against conspiracist-extremist appeals might be effective (Banas and Miller, 2013; Braddock, 2019).

Our approach needs to become part of, but also go beyond, preventing violent extremism (PVE) strategy and programming. Policy settings need to redress:

- The post-truth environment in which conspiracist thinking flourishes

- The economic inequalities that fuel its potency

- The social divisions that nurture its narratives

- The technological affordances that drive its dissemination

All of these are critical areas of investment in mitigating how violent extremist movements can weaponise COVID-19.

....

Michele Grossman is Professor and Research Chair in Diversity and Community Resilience, Convenor of the AVERT Research Network and Director of the Centre for Resilient and Inclusive Societies at Deakin University in Australia. Her research focuses on how to build resilience to and engage communities in preventing violent extremism.

NATHAN SMITH & EMMA BARRETT

LESSONS FROM A RAPID RESPONSE

Tasked with supporting the stress resilience, performance, and health of frontline workers during the initial response to the COVID-19 pandemic, Dr Nathan Smith and Professor Emma Barrett discuss how their rapid response process can be applied to the work of security practitioners facing similarly demanding situations in the future.

Many security, policing, and military environments expose workers to chronic pressure. Security personnel must juggle competing demands under time constraints, working out how best to deploy scarce resources (time, skills, and equipment) to achieve optimal outcomes. Their lives and those of civilians are often at stake, threatened by unpredictable adversaries of uncertain capability and ambition. And then, sometimes, unexpected events occur that escalate and intensify this pressure such as the 2001 al-Qaeda attacks in New York or the Taliban's swift takeover of Afghanistan in 2021.

Although not a security threat in the traditional sense, the early stages of the COVID-19 pandemic is a vivid example of a highly stressful and unexpected event. As enormous pressure was placed on healthcare systems around the world, frontline workers were quickly identified as being at increased risk of extreme stress and trauma exposure.

The psychological impact of novel, uncertain and traumatic events can be extraordinarily difficult to manage. Such situations often require a rapid response, whilst acute pressure piles on top of chronic pressures, in the glare of intense public scrutiny. But existing skills and previous training may be insufficient to respond to these new events.

Surge personnel – often inexperienced and under-trained – may need to be assimilated into existing teams. Standard operating procedures may prove ineffective and contingency plans may not be robust or even be non-existent. In these circumstances, personnel are forced to cope as best they can until effective plans can be implemented, sometimes for weeks at a time, often in the face of extraordinary human suffering, trauma, and death. How do workers cope with such novel, uncertain, dynamic, traumatic, and life-threatening sources of stress? How can

> **" Personnel are forced to cope as best they can until effective plans can be implemented, sometimes for weeks at a time, often in the face of extraordinary human suffering, trauma, and death.**

their organisations best support them? And how can existing behavioural science research help in the face of acute pressures?

In this article, we describe some of the processes we followed and the lessons we learned. We discuss how these lessons can be applied to the work of security practitioners facing similarly demanding situations in the future.

RAPID RESPONSE

Early in 2020 we were contacted by those coordinating the NHS's COVID-19 response to develop a 'Just-in-Time' training and education curriculum to support frontline workers. The aim was to share the most up-to-date evidence and best practice related to ensuring the resilience, performance, and psychosocial health of frontline staff. Those coordinating the pandemic response quickly realised that it would force healthcare workers to operate in an entirely unfamiliar context. This was particularly the case for support staff being drafted in to fill gaps in healthcare provision and/or to provide relief to those key workers that were having to self-isolate after contracting the virus or symptoms.

Image credit | Cryptographer / Shutterstock.com

Speed was critical to meeting these requirements. When they contacted us prior to the first national lockdown in March 2020, the NHS response team estimated they had approximately two weeks before a surge in hospitalised cases. This two-week window was an opportunity to establish ways of working that would contribute to resilient function, optimise performance and protect staff from mental ill-health in the weeks and months ahead.

The message was clear: quality materials needed to be produced quickly if they were to be helpful and make a meaningful contribution. This demanded a balance between expediency and quality (Figure 1). Poor quality materials produced quickly were likely to be ignored by frontline workers ('non application') or risked giving harmful advice. Materials rigorously but slowly produced risked being applied at a late stage ('delayed application') and not meeting potential users' needs. We needed to work at pace but put in place assurance processes that helped us to ensure quality and to produce work that was operationally useful.
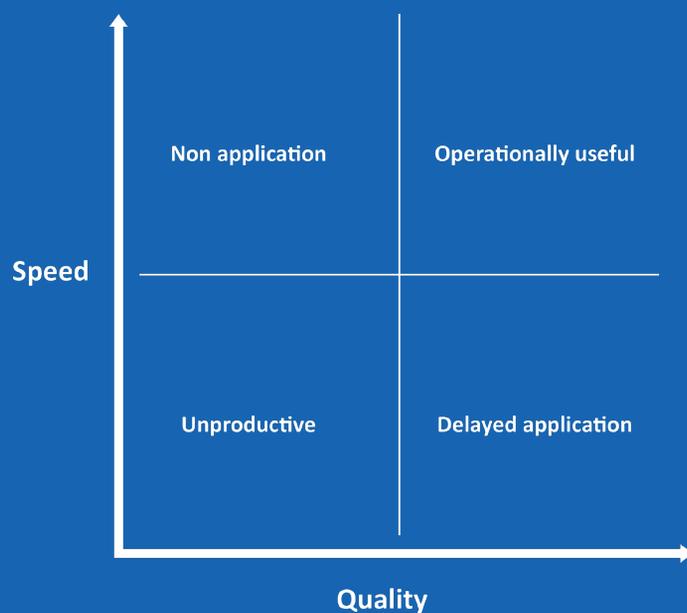

Figure 1: Matrix capturing the balance between expediency and rigour for producing operationally useful material in crisis response.

> ## "The early stages of the COVID-19 pandemic have much in common with novel, unexpected security events, and we believe that the lessons for frontline personnel are very similar.

Our approach is presented in a rapid reaction model in Figure 2. We started by working with the NHS response team to identify their specific user requirements to ensure that what we produced was of genuine value to frontline workers. To ensure quality, we reached out to an expert consortium of academics and practitioners to establish an informal working group. Members of this group both wrote material and provided peer review of our and each other's work. This was an essential step, providing a layer of quality control that gave credibility to our work. Through their invaluable hard work and expertise, peer review of material happened at pace, generally within 24 hours.

Our outputs focused on how to engender resilient function at individual, group and organisational levels. We produced a series of evidence-based briefing notes that were directly informed by the requirements of end users. These covered topics including PTSD, moral injury, managing extreme stressors, understanding resilience, motivation, leadership, performance debriefing, readiness to work, decision making, team dynamics, fear of failure, isolation, and organisational culture. We worked with the NHS team to identify what communication and products would be most helpful. The requirement was for a series of briefs, that set out a clear rationale for the relevance of the subject, offering practical recommendations to complement rather than replace existing knowledge.

The design support was invaluable to ensure the briefing notes were clear and engaging. Notes were produced in both printable form and uploaded to a website (www.supporttheworkers.org) and we placed no restrictions on sharing. The notes were quickly shared throughout the UK (with the NHS and others involved in responding, such as military and security) and internationally (with the World Health Organisation and Johnson and Johnson Institute).

Amid a fast-moving operational response, we found it tricky to carry out a formal evaluation of the impact of our work. Our approach was to gather immediate feedback from the NHS team that tasked us on how the materials were being received at the frontline, which provided an opportunity to adjust and iterate our approach when developing additional resources. The feedback was gratifying, for example: *"a collaboration of immense value and rigour in keeping us all grounded in best practice but without slowing our response ability down."*

LESSONS FOR SECURITY

We draw two key lessons from this activity. First, it is essential that materials produced during crises, such as during the response to a terrorist incident or fast-changing diplomatic situation, are both shaped by end-user needs and designed for that audience. Resisting the urge to spring into immediate action and instead taking time to speak to a range of end users will help ensure materials produced are relevant and fit for purpose – as long as such consultation can be done quickly.

Second, we have shown it is possible to produce a response that is both rapid and of high quality. Confirming response timeframes is crucial for effectively communicating and managing expectations of both end users and experts. Much can be done in a very short space of time if people are committed and conscious of the time pressure. In our case, two weeks was enough to access available expertise and evidence and to put in place robust and rapid peer review processes.

In terms of the acute stressors placed on frontline personnel, the early stages of the COVID-19 pandemic have much in common with novel, unexpected security events, and we believe that the lessons for frontline personnel are very similar. Indeed, some of the evidence we drew on for our briefs was derived in security settings. Our briefs may therefore be of value to security personnel with minimal editing. However, novel circumstances may arise in future that demand additional or different research briefing notes and we suggest that the rapid response approach we adopted for COVID-19, and in particular focusing on end user requirements and maximising the opportunity for evidence-based practice, may provide useful direction for security practitioners responding to significant events in their work.

....

Dr Nathan Smith is a Research Fellow in Psychology, Security and Trust at the University of Manchester.

Emma Barrett is Professor of Psychology, Security and Trust in the Department of Criminology at the University of Manchester. She is also Director of SPRITE+ the EPSRC Digital Economy NetworkPlus for Security, Privacy, Identity and Trust. Her research interests include new technologies and crime, betrayal and trust, and performance in extreme environments.
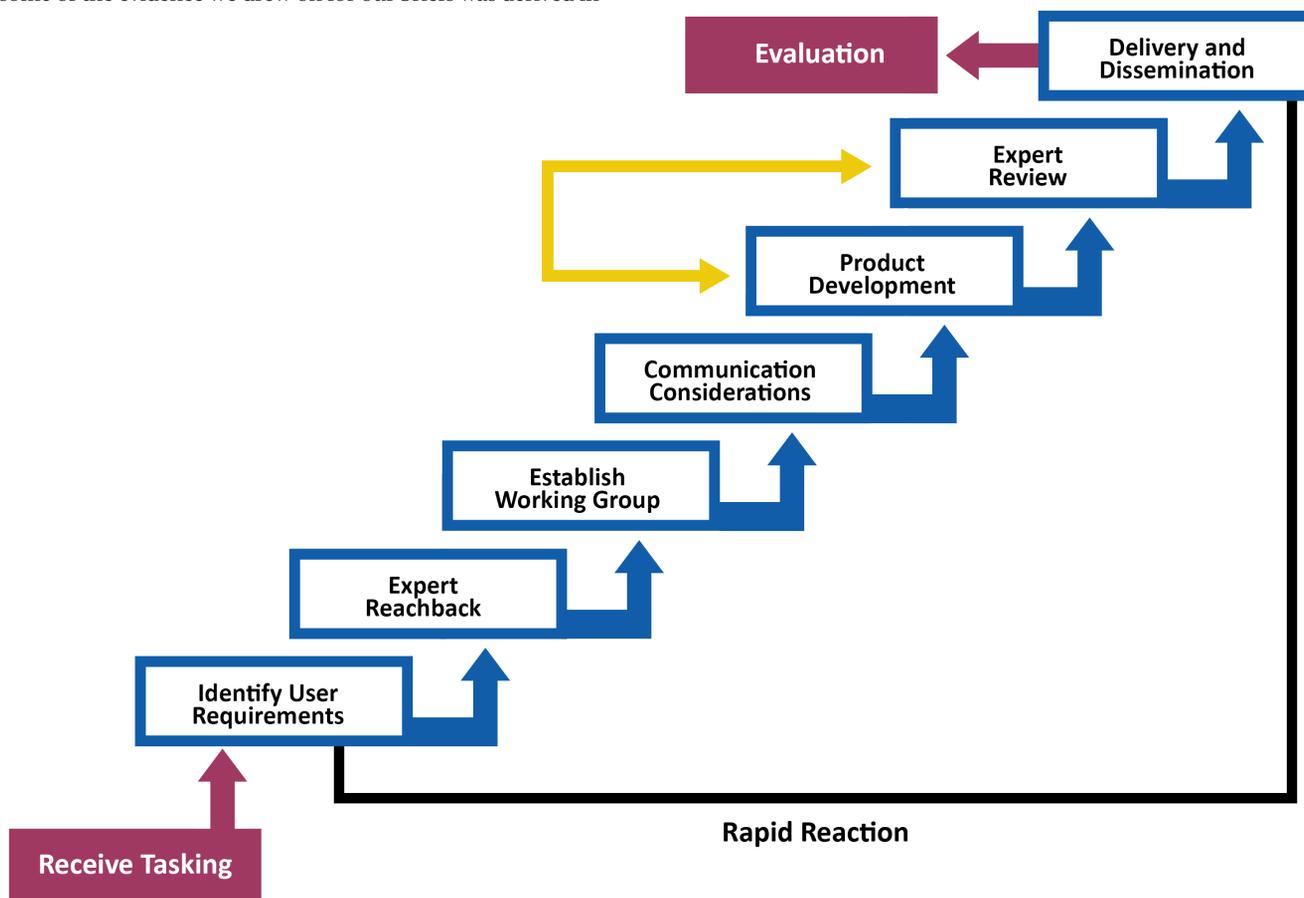
Figure 2: Rapid reaction model used to guide product development during COVID-19 response.

LORRAINE HOPE, RACHEL ZAJAC, & MARYANNE GARRY

WHERE WAS I LAST WEDNESDAY?

Why contact tracing needs a dose of memory science.

In the battle against COVID-19, we have few weapons. Even as vaccines roll out, countries are still struggling to contain the outbreaks that burden healthcare systems and impede economic recovery. Technology, heralded early on as the 'silver bullet,' has offered limited benefits. Contact tracing—the century-old process by which public health officials identify those who have been exposed to infection—remains among the most powerful tools for containing outbreaks. However, its success is variable.

To cognitive scientists, this comes as no surprise. Contact tracing's ability to break the chain of transmission is only as good as the information that interviewed cases provide. And hidden in the variable that a contact tracing model might call 'completeness' is another weak link in the chain: human memory. To scientists of memory, contact tracing needs to gather complete, precise, accurate information from witnesses to an ill-defined event. Contact tracers, therefore, face the same challenges as their witness-interviewing counterparts.

WITNESSES UNWITTINGLY OMIT INFORMATION

The frustrating reality of contact tracing is that retrospective importance and urgency are unlikely to translate into better recall. Many of the locations we move through, the activities we engage in, and the encounters we have, are entirely mundane. We go to the gym, buy groceries, pick up a pizza, meet friends and colleagues. These situations—and even the riskiest among them—are simply the backdrop of our daily lives. Without arousal, salience, and emotion to engage processes that prioritise attention and enhance memory, many of these events are unlikely to feature in our recollections.

Omitted information presents the greatest challenge for contact tracing. Failure to recall a single event can mean that an unidentified person (say, a neighbour we spoke to briefly) or unidentified people (say, the other people at the cinema) can unknowingly transmit the virus.

Contacts can also be lost when interviewed cases fail to recall symptoms. Someone might remember waking up short of breath on Thursday but neglect to report feeling unusually tired since Monday—a small omission leading to three days of missed contacts. Finally, our memories can be imprecise, so even when people recall relevant behaviour, there is no guarantee they will provide adequate detail.

> "Someone might remember waking up short of breath on Thursday but neglect to report feeling unusually tired since Monday—a small omission leading to three days of missed contacts.

WITNESSES MAKE MISTAKES

Memory reports are not only notoriously incomplete, they are also notoriously error-prone. Some of these errors occur when people over-rely on what usually happens ("On Fridays, I usually go to the movies"). People also make errors when they fail to distinguish what they experienced from information they encountered somewhere else.

People can even combine details of several genuine events; these faulty recollections can be particularly easy to mistake for real experiences, because their components all really happened—just not together as a single event.

WITNESSES HAVE VULNERABILITIES

Even when operating at an optimal level of cognitive capacity, people's memory for incidental information is typically poor. But many witnesses are not operating at that level—whether due to young or old age, limited intellectual functioning, mental distress, or other factors. In this pandemic, interviewed cases may be unwell and in pain. Pain disrupts performance on various cognitive tasks, and acute illness—including viral infection—is associated with impaired executive function and

working memory. Impairments like these might hinder cases' ability to recall details or even to engage in the retrieval activities necessary to remember those details.

WITNESSES CAN BE RELUCTANT

Successful interviews depend on people's willingness and motivation. Yet, for numerous reasons, interviewed cases might not be fully cooperative. They might have limited understanding about the utility of the information they provide or lack faith in the contact tracer or agency involved. They might not want to share private or sensitive information—perhaps because they are worried about how, when, and by whom that information will be used. Most pragmatically, they might be concerned about the consequences of speaking to a contact tracer about their personal wellbeing and livelihood, particularly if required to self-isolate for an extended period.

WHAT CAN HELP?

Although contact tracing is one of the main COVID-19 infection-control strategies available, standardised contact tracing protocols—that are informed by memory research—are strangely absent. Guidelines from agencies such as the WHO or the CDC correctly emphasise the need to obtain an exhaustive list of contacts, but provide little to no guidance about methods to achieve this. Thus, in the case of COVID-19, we know the 'what' but the 'how' is much less clear.

The good news is that we already have a considerable body of empirical and applied literature that provides a framework for increasing the completeness and accuracy of the information we obtain from people.

Our challenge now is marshalling expertise and resources, so we are ready for what comes next.

....

Lorraine Hope is a Professor of Applied Cognitive Psychology at the University of Portsmouth. Her research focuses on applied memory performance and the development of tools and techniques, informed by psychological science and practitioner context, for eliciting information and intelligence across a range of investigative contexts.

Rachel Zajac is a Professor of Psychology at the University of Otago, New Zealand. Her research focuses on children's and adults' eyewitness testimony, social influences on memory and decision-making, and biases in the interpretation of forensic evidence.

Maryanne Garry is a Professor of Cognitive Psychology at the University of Waikato. She has amassed a body of theoretically grounded applied research that sheds light on the causes and consequences of false memories. She also studies how memory fades or becomes distorted.

Photo by Towfiqu barbhuiya on Unsplash

11

JORDAN NUNAN & IAN STANIER

INTELLIGENCE GATHERING DURING A PANDEMIC

How did informant handlers adapt to the measures implemented during the COVID-19 pandemic, and what was the consequence on their capability to optimise intelligence from informants?

In response to the COVID-19 pandemic, the Government introduced measures (national lockdowns and regulations) restricting people's movements, their access to premises, and limitations on people's social and professional association through the application of physical distancing rules. Dr Jordan Nunan and Dr Ian Stanier investigated practitioners' perceptions of the impact of the COVID-19 pandemic on Dedicated Source Unit's (DSU) ability to elicit intelligence from informants.

THE NEED TO ADAPT

Organisational adaptation requires senior leaders to make informed decisions drawn from its corporate memory. Corporate memory and its subsequent decision-making capability are informed through peer-reviewed research, continuous professional development, problem solving and operational practices. In the context of informant management, this includes Authorising Officers (AOs) and the National Police Chiefs' Council (NPCC) leading strategic steering body for United Kingdom informant policy: the National Source Working Group (NSWG).

The pandemic offered an opportunity to accelerate organisational adaptation to address emerging challenges, including:

- Safe and secure digital information between informants and handlers

- Remote access to sensitive databases

- Electronic payments

- Enhancing the use of online communication (including recruitment and tasking).

Many of these challenges pre-dated the outbreak of COVID-19 but the pandemic brought the operational and organisational requirements into sharper focus.

There are incentives to adaptation. For example, securing a satisfactory solution to electronic payments may be organisationally beneficial. Electronic reward payments may reduce the need for physical contact and therefore reduce risks of COVID-19 transmission. The method offers opportunities to reduce informant-handler compromise while travelling to, from and at meeting venues. Electronic payments provide a digital audit trail and offer a degree of corruption-proofing in financial transactions and speed up the reward process, which may enhance the handler and informant trust and confidence.

On the other hand, cash payments may offer an opportunity to personalise the interaction, to assess the informants' welfare and to maintain rapport, which depersonalising and clinical financial transactions may not. The audit trail of digital transactions may also risk compromise of the informant-handler relationship.

INSIGHTS THAT WILL BETTER PREPARE INFORMANT MANAGEMENT

The experiences of operators, distilled from their exposure to operating at the peak of the pandemic, are useful. They can inform the development of good organisational practices, offering opportunities for greater operational resilience. Some of the key findings from our conversations with informant handlers are listed below:

Health protection

- Access to the appropriate health protection measures (e.g., vehicle adaptation, venue selection and PPE) is needed to maintain physical meetings.

- The pandemic reinforced the fact that the physical and mental welfare of the informant is as important as the collection of intelligence.

Governance

- To ensure business continuity, operators seeking to manage risk may have to accept the 'least-worst' decision. However, with creative practice and informed leadership, risk mitigation is always possible.

- Decision inertia must be challenged, with presumed risks correctly substantiated and proactively managed.

- Policy and practice development should avoid an overly cautious approach regarding ongoing use and management of informants.

- Traditional organisational approaches to policy development need to be reviewed in the context of its ability to respond to dynamic and extreme operational events.

Innovation and technology

- Informant management needs to accelerate technology adaptation and adoption where extant practices fail to maintain operational capabilities. Technology offering clear improvements over pre-pandemic practice should be more widely adopted.

- Organisational culture needs to quickly embrace technology and new ways of working. In wider society, the pandemic acted as an accelerant in the adoption of technologies, including online virtual meetings, online purchasing, and electronic banking.

Recruitment, communication, and informant development

- Automatic cessation of recruitment efforts during a pandemic is rarely justified. A decision to recruit an informant should be on a case-by-case basis and centred on the individual circumstances.

- Where there are restrictions on traditional communication methods (face-to-face meetings) greater consideration should be given to utilising secure digital communication platforms.

- Existing recruitment strategies should be agile enough to address new types of criminality and emerging trends associated with the pandemic (i.e., counterfeit PPE, online fraud, and burglary artifice by posing as medical staff).

Tradecraft and intelligence

- The collection of intelligence during the restrictions fell significantly in terms of quantity and quality. This was commensurate with falls in overall reported crime.

- Government COVID-19 restrictions on movements has the unintended consequence of restricting traditional handler-informant meetings. In response, handlers developed their tradecraft leading to an increase in alternative methods of communication, including dead letter drops and brush contacts.

- New and innovative tradecraft practices developed during pandemic related restrictions should be captured and shared throughout the informant handling community.
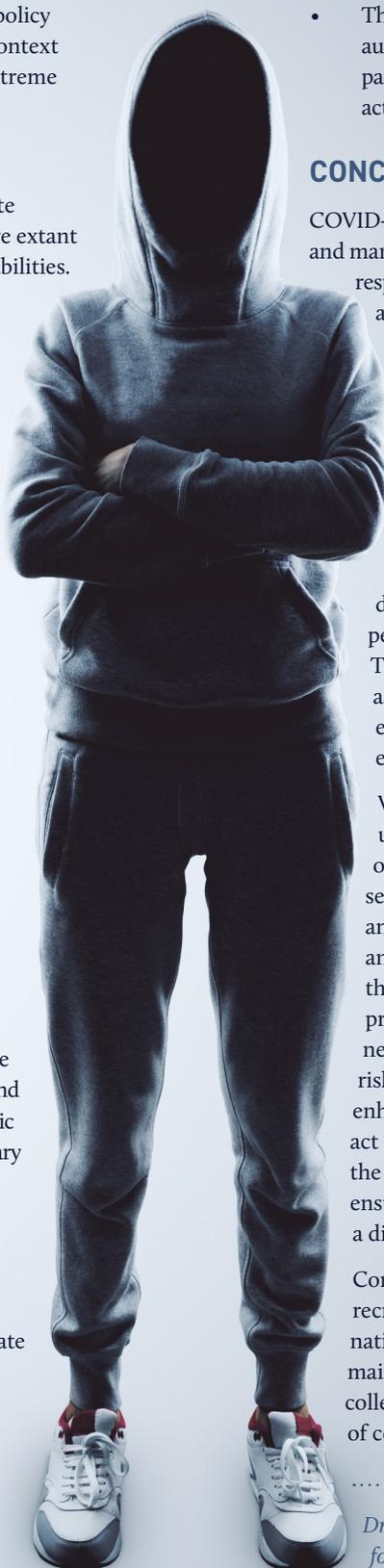
- The primary purpose of the recruitment and authorisation of informants, even during a pandemic, continues to be the collection of actionable intelligence.

CONCLUSION

COVID-19 acted as an inflection point for the use and management of informants. Consequently, the response to the pandemic demanded organisational adaptation on a scale not witnessed since the enactment of the *Regulation of Investigatory Powers Act 2000*. Accordingly, future informant use needs to be capable of responding to unexpectedly extreme environments.

This critical responsibility remains a primary purpose of strategic leaders who need to quickly respond, review, and adapt existing policy and practice, by setting the direction, developing the organisation and its people and a readiness to take informed risks. This requires an acceptance that not all risks associated with informant use can be eliminated, especially as keeping the informants in play is essential.

What are the lessons to be drawn? During unexpected events and rapidly changing operating environments, it is critical that senior leaders encourage the capture, recording and access to operationally critical knowledge and experience. In the case of informant use, these include additional exploration of how practitioners may further utilise existing and new secure remote access capabilities, to reduce risk, maintain professional relationships and enhance efficiencies. Governance and policy must act as enablers to necessary change. This includes the adaptation and adoption of new practices, to ensure a measured response to perceived risks and a disposition to amend long-standing policy.

Corporate memory will enable the continued recruitment of informants during periods of national emergencies. It will assist with the maintenance of effective relationships, the collection of relevant intelligence and the delivery of community safety.

Dr Jordan Nunan is an Associate Lecturer in the forensic elicitation of intelligence at the Liverpool Centre for Advanced Policing Studies (LCAPS) at Liverpool John Moores University.

Dr Ian Stanier is a Senior Lecturer at LCAPS at Liverpool John Moores University.

LIV BROWN

MULTI-AGENCY EMERGENCY RESPONSE

Large-scale emergencies such as the global COVID-19 pandemic, terrorist attacks, and environmental disasters require the coordinated efforts of several specialised and diverse teams.

Multi-agency emergency response teams are characterised as multi-team systems – that is, multiple component teams, each tasked with their own agency-specific priorities while simultaneously working towards shared overarching goals. For example, in a terrorist incident, all responders will be focused on saving life and reducing harm. However, each agency will also be working towards their own priorities – the Police are tasked with mitigating further threats (cordoning off the scene and collecting evidence), while the Ambulance service must quickly begin accessing and triaging casualties.

In practice, multi-agency working can present several challenges. For example, which agency's goals take precedence if there is a conflict in priorities? And how can effective communication across agencies be maintained when there are urgent tasks to attend to?

In the UK, several underlined initiatives were introduced to overcome the challenges associated with inter-agency working. However, as highlighted in the report reviewing the Manchester Arena terrorist attack, poor communication and difficulties managing collaboration across agencies continue to permeate the response to complex emergency incidents.

RESEARCHING EMERGENCY RESPONSE TEAMS DURING A SIMULATED TERRORIST INCIDENT

In light of the ongoing challenges to multi-agency teamwork during emergencies, our research examined key team processes: communication and coordination during the strategic response to a simulated terrorist incident. The simulation was based on the response to a terrorist attack involving firearms at a shopping centre in the run-up to Christmas. Data collected from 30 senior commanders represented 11 agencies including Police, Fire and Rescue, Ambulance Service, Military, Local and Central Government, and the Red Cross.

A key element to our research was to examine how responders communicated and coordinated at different simulated time points in the incident response. Existing government guidelines state that the response to incidents is structured in two phases

– the Response Phase (neutralising the threat, saving life, and protecting the community) and the Recovery Phase (rebuilding trust in the community, supporting victims in the longer term, and helping to 'restore normality'). However, no empirical research has tested if the dichotomisation of Response/Recovery works in practice.

To address this, our study measured responders' behaviour at three simulated time points, with each time point classed as either Response or Recovery within government guidelines:

Phase 1: Incident ongoing (Response)

Phase 2: 48 hours after the incident (Response)

Phase 3: 3 weeks after the incident (Recovery)

Communication was measured through social network analyses. We used audio recordings of the simulation to generate communication networks and identify which team members communicated with one another and how frequently.

Coordination was measured by qualitatively coding the transcribed audio recordings to identify verbal indicators of coordination. For example, joint decision-making was indicated by team members actively working together to implement a decision, e.g., "Can I confirm that we all agree on this strategy before it is actioned?"

Based on existing government guidance, we expected to identify differences in how the teams communicated and coordinated in the response phases (Phase 1 and 2) and the recovery phase (Phase 3).

WHAT WE FOUND

In Phase 1 of the response, the communication network was highly centralised, with much of the information being shared by the Police. While it is usual for the Police to take charge of incidents that involve firearms, the data suggest that an over-reliance on the Police to maintain communication across the network led to coordination difficulties in this phase. The results suggest the Police were so focused on delivering the overall

> "In rapidly developing crises, boundary spanners can communicate evolving plans quickly to ensure safe practice and a cohesive approach across inter-agency partners."

strategy of the response that they failed to attend to important information provided by other agencies and to manage the flow of communications across the network . This ultimately disrupted coordination as marked by delays and uncertainties in implementing decisions.

As the incident evolved across the simulated time points, the involvement of additional agencies increased and the communication networks became less centralised. The changes to the communication networks coincided with improved coordination across agencies as marked by increased joint decision-making, shared awareness, and reduced conflict and uncertainty.

Given the high cognitive load on central agencies (e.g., the Police) in the immediate aftermath of incidents, decentralised communication networks might be introduced earlier to make better use of the diversity of expertise across agencies and increase coordinated action.

HOW CAN WE IMPROVE MULTI-AGENCY WORKING UNDER PRESSURE?

Implementing boundary spanners

Mapping the communication networks demonstrated a disconnect across agencies and a reliance on central commanders to manage the flow of information and implement key decisions. One solution is to introduce "boundary spanners": specific team members tasked with ensuring that information is relayed and actions are coordinated across

agencies. Boundary spanners have the potential to reduce the load on central decision-makers and allow information to be transferred more easily between team members. In rapidly developing crises, such as the early stages of the COVID-19 pandemic, boundary spanners can communicate evolving plans quickly to ensure safe practice and a cohesive approach across inter-agency partners.

Introducing an additional phase

Our results showed a three-phase structure of "Response–Resolve–Recovery" more accurately described the behaviours of responders during emergencies than the existing "Response–Recovery" structure outlined in government guidelines. Implementing an additional phase would account for the shift in urgency between an ongoing incident (Response) and shortly afterwards when the immediate threat has subsided (Resolve).

Changing procedural guidelines to a three-phase structure may better prepare responders for the realities of incident response and empower other agencies to be involved in the decision-making before the response transitions into the recovery phase. This would increase opportunities for collaboration across agencies and reduce the load on central agencies, such as the Police.

....

Dr Olivia Brown is a Research Associate at the University of Bath. She is interested in how intra- and inter-group processes influence individual and group behaviour.

STEPHAN LEWANDOWSKY & MUHSIN YESILADA

THE "INFODEMIC", INOCULATION, AND INSURRECTIONS

A COVID-19 vaccination communication handbook has been published to tackle misinformation, providing specific hints about how to communicate the vaccines.

The COVID-19 pandemic has changed everything. It has disrupted global travel and the economy, and public health responses to the pandemic have curtailed democratic freedoms to an unprecedented degree in most western countries. The pandemic has also been accompanied by an "infodemic" of misinformation and conspiracy theories. In the UK, around 1 in 4 adults believe in at least one conspiracy theory relating to COVID-19.

Conspiracy theories and misinformation have demonstrable adverse consequences because they hinder our ability to respond effectively to a crisis. For example, exposure to misinformation has been shown to reduce people's intention to get vaccinated by 6% or more.

Given that widespread vaccination is a key ingredient to help the world recover from the pandemic, the effect of anti-vaccination misinformation is particularly concerning and renders communication about the COVID-19 vaccines – and encouraging vaccine uptake – particularly critical. To assist with this, an interdisciplinary team of more than 25 scientists worldwide has recently published a COVID-19 vaccination communication handbook. The handbook is freely available for download in 11 languages and provides specific hints about how to communicate the benefits of COVID-19 vaccines. It is aimed at all types of practitioners, from physicians and nurses to journalists and people in government, but also the public at large.

INOCULATION

One of the techniques to combat misinformation that is explained in the handbook involves inoculation of the public against misinformation, ideally before it is encountered. To inoculate people involves two steps:

1.   A warning that they may be misled.

2.   A pre-emptive refutation of the misleading argument.

Inoculation thus follows the biomedical analogy: By exposing people to a weakened dose of the techniques used in misinformation and pre-emptively refuting them, "cognitive antibodies" can be stimulated.

Inoculation has been successfully used against COVID-19 misinformation. In one study, people played a video game, called GO VIRAL! that trained players in creating viral misinformation using common misleading techniques. Learning how to create misinformation enabled people to detect when they were being misled after they finished playing the game.

Interestingly, inoculation has been shown to work across several domains, including political radicalisation. In one of our recent studies, participants were shown a video about how to identify misinformation techniques commonly used in Islamophobic and radical-Islamist material. Following this inoculation treatment, participants either watched an Islamophobic video or a video conduit to radical Islamist content. Both videos contained numerous items of misinformation. Individuals who received the inoculation displayed less agreement with the misinformation, demonstrated less sharing likelihood, and had less support for the misinformation. The results are encouraging because they show that inoculation can help combat extremist messages, a terrain that is usually considered very challenging.

The inoculation strategy was also effective without having to refute a specific incident of Islam-related disinformation. The virality and evolving nature of disinformation often make creating a catered rebuttal difficult, and the rebuttal may fail to reach the consumers. Thus, the notion of an intervention that combats disinformation without directly addressing specific examples of disinformation is encouraging.

The success of inoculation is not the only link between COVID-19 misinformation and radicalising material about Islam: both types of misinformation also have implications for national security. In the case of Islamophobia and radical Islamism, the impact on national security is immediately obvious. In the case of COVID-19, the implications are less clear but arguably also profound, as discussed next.

BLENDING OF CONSPIRACIES

Across Europe, the pandemic was instrumentalised by the far right to push a strong nativist narrative, linking the pandemic to immigration, immigrants, and ethnic minorities. Far-right opposition parties in Europe also opposed any mandatory COVID-19 public-health measures, from mask-wearing to social distancing to COVID-19 tracking apps, largely based on misleading or outright false information.

Conspiracy theories about COVID-19 and the vaccines have now also become intertwined with QAnon. QAnon is a conspiracy theory that originated in 2017 on far-right chat sites in the US but has now moved closer to the mainstream and is spreading across the globe.

Although QAnon defies easy description, its core tenet is the allegation that a cabal of Satanic, cannibalistic paedophiles is operating a global child sex trafficking ring and conspired against former President Trump while he was in office. In May 2021, 15% of Americans endorsed at least one of three of the main claims of QAnon, confirming the attractiveness of the theory to a notable share of the population. QAnon has been identified as a national security risk by the FBI, and its adherents played a focal role during the violent insurrection at the US Capitol on 6 January 2021.

From early 2021 onward, anti-vaccination conspiracy theories have become increasingly prominent within the QAnon ensemble of baseless and easily disproven claims. The growing links between the far-right QAnon milieu and anti-vaccination conspiracies are not limited to the US. In Germany, for example, QAnon has close links to the so-called Querdenker movement, an umbrella term for people who oppose all aspects of COVID-19 public-health measures, from masks to social distancing to

> "In the UK, around 1 in 4 adults believe in at least one conspiracy theory relating to COVID-19."

vaccinations. Querdenker members often ally with the extreme right, and their demonstrations often end in violence.

Pandemics have given rise to conspiracy theories for centuries. When people suffer a loss of control or feel threatened, they become more vulnerable to believing conspiracies. Pandemics also lead to major social change, and in the case of COVID-19, to restrictions on people's civil liberties and freedoms. It is thus unsurprising that those two strands of consequences of pandemics should become intertwined.

The blending of political conspiracies and pandemic-related conspiracies is therefore also not entirely surprising. Given the clear potential for violence in the extreme-right conspiracy milieu, conspiracy theories relating to COVID-19 therefore also have national-security implications.

....

Professor Stephan Lewandowsky is Chair in Cognitive Psychology at the University of Bristol. His research focuses on misinformation and how the pressure points between human cognition and social media affect democracy.

Muhsin Yesilada is a Doctoral Researcher at the University of Bristol. His research explores how inoculation might safeguard people against radicalising messages online.

LAURENCE ALISON, EMILY ALISON, SARAH ROBERTSON & MICHAEL HUMANN

THE GROUND TRUTH AFTER-ACTION REVIEW TOOL

The after-action review tool Ground TRUTH helps prepare for, adapt to, and recover from critical incidents.

Psychologists and military personnel developed the Ground TRUTH After-Action Review tool in March 2020. Drawing on research on what works in after-action reviews, and written by authors with research backgrounds in critical incidents and counselling as well as operational experience, the tool supports adaptive recovery in the intense operational and chronic environment of COVID-19.

Research into debrief approaches has demonstrated that after-action reviews enable users to understand and cope with challenges they face, as well as discuss performance and identify plans for improvement. The Ground TRUTH tool was developed in response to a call from the NHS to help support staff and maximise operational capacity during the COVID-19 pandemic. Here, the authors provide an overview of the tool and its application.

The Ground TRUTH tool aims to:

1. Feedback important observations from the 'ground up' to shape decision-making.

2. Prevent burnout by monitoring fatigue, improving stress awareness, and boosting coping.

3. Develop shared understandings by identifying learning fast and improving team morale.

4. Be easy, rapid, and efficient, with its deployment as frequent as it was helpful (usually weekly) and brief (sometimes only seven minutes, more often 20). Data had to be easy to manage and easy to interrogate.

There were many successes with the tool deployed across over 50 social care, health, and emergency services, as well as military settings. One notable success was at Alder Hey Children's Hospital, which had to adapt to caring for adult patients with COVID-19 in response to pandemic pressures.

Working with Dr Sarah Robertson (Clinical Psychologist) in the Staff Advice Liaison Service and Organisational Development, we carefully monitored outcomes.

Feedback from a two-phase implementation found 98% of staff said the tool was helpful, with one-third of staff reporting feeling better after reflection and nobody reported feeling worse.

This feedback led to Trust Executives at Alder Hey supporting an organisation-wide implementation with a regular TRUTH slot at their monthly strategic meetings. The Communications Department disseminated targeted and solution-focused in Trust-wide briefings and TRUTH bulletins. This activity led to the Health Service Journal award for Staff Engagement within their 'flourishing in adversity' program.

The tool is not intended to identify and monitor mental ill health but is aimed at increasing awareness (of self and others in teams), supporting all staff to proactively monitor and boost coping. These insights improve shared situational awareness among teams while also feeding directly up to team leaders and managers, enabling them to respond more effectively to needs and requirements on the ground.

THE FIVE STAGES OF TRUTH

1. **T**alk and log the issue – 'What was difficult?' (negative) and 'what worked well?' (positive).

2. **R**eview management of the issue, preferred outcomes, and 'making tomorrow a better day' for the organisation.

3. **U**nderstand what can be learnt from the event – this is goal-directed and future-leaning, asking why this happened and what we can learn.

4. **T**ell others and the organisation what is needed to improve responses.

5. **H**eal and move forward – focusing on reducing stress, improving morale, health and wellbeing.

We adopted a self-initiated approach utilising active listening, authenticity, and compassion. With regards to the therapeutic principles enshrined within the tool, we were:

- **Non-directive:** the tool is user-led and provides prompts to encourage reflection.

- **User-centred:** the user is always the best person to resolve issues; the tool enables user-centred learning.

- **Positive:** the user builds resilience through self-empowerment.

Data is hosted on an online platform that can be used by individuals alone, in pairs, or in groups. Data can be extracted to create outputs for teams. Outputs include summaries of categorical data related to issues, successes, goals, learning, and average morale and coping. Outputs can be shared with TRUTH leads, line managers, and strategic leads.

Leads can utilise the information to enhance existing infrastructure, such as in team meetings, supervision, debriefs, and reflective spaces, accelerating the ability to get teams to gain a fuller shared picture (Mathieu et al, 2000). Reports are shared via email and in posters in clinical areas. Decision-makers respond with key actions in the form of a TRUTH bulletin. Themes are used to shape the offer of staff support responsively and proactively.

Because of the specific success at Alder Hey and increasing demand across the health sector, we are now working with Alder Hey to form a TRUTH team to produce guidance, manuals, and materials that will feed into a comprehensive toolbox. We are also supporting launches in similar healthcare settings, as well as military and disaster-response organisations.

The key to the tool's success was recognising that during fast-moving, high-stakes, and chronic critical incidents, psychological support needs to be rapid, efficient, and responsive to the operating environment. There is no luxury of time to support staff, nor the need nor utility (during 'the storm' itself) for lengthy unpicking and discussion of stress and trauma.

To support staff in such high-stakes environments and enduring times of stress, we need to recognise tempo, bandwidth, and the importance of listening. Working within the staff's 'window of tolerance' to identify and remove obstacles can support adaptive recovery at an individual and organisational level, improving people management, human performance, and reduced sickness.

Professor Laurence Alison is the Director of Ground Truth, a research and training consultancy for military and law enforcement leaders.

Emily Alison is a Behavioural Consultant Psychologist and has been involved in the development of the Preventing Violent Extremism Tool for profiling potential extremism and the ORBIT framework.

Dr Sarah Robertson is a Clinical Psychologist at Alder Hey Children's Hospital, applying psychology at an organisational and individual level to staff support.

Dr Michael Humann develops and delivers training using immersive simulated learning environments, aimed at improving critical incident decision making and developing expertise in policing and emergency response.

"Feedback from a two-phase implementation found 98% of staff said the tool was helpful, with one-third of staff reporting feeling better after reflection and nobody reported feeling worse."

Photo by Luke Jones on Unsplash

JASON R.C. NURSE

BALANCING CYBERSECURITY & PRIVACY IN THE REMOTE WORKFORCE

Remote working will only truly work if we get the balance of security and privacy right.

The COVID-19 pandemic took the world by surprise and countries are still grappling with its impact on society, the immense loss of life, and how to return to any form of normality. As remote working increased during the pandemic, so too did the cyber-attacks aiming to exploit it.

Malevolent actors viewed the pressures caused by the pandemic as the perfect opportunity to launch a variety of cyber-attacks. These targeted critical national infrastructure (e.g., ransomware and intellectual property theft attacks on healthcare and medical research organisations), businesses (via their remote workforces and often newly-adopted distributed working infrastructure), and members of the public (using a range of coronavirus-related scams) (Lallie et al., 2021). En masse, these attacks proved substantial and forced governments and organisations to rethink their approaches to cybersecurity.

Unfortunately, many issues remain for securing the post-COVID-19 remote workforce and balancing cybersecurity and privacy going forward.

SECURING TODAY'S REMOTE WORKFORCE POSES A NEW AND DIFFERENT CHALLENGE

Before COVID-19, working from home was a carefully managed reality typically reserved for those who had specific jobs, were at a prescribed level of seniority or had extenuating circumstances. In general, these individuals were trusted by the employer and were trained (either directly or via previous experience) in working effectively and securely from home. COVID-19, however, changed this situation considerably, with millions of new workers suddenly forced to work remotely with little training and in challenging home and personal environments.

My research, with colleagues (Nurse et al., 2021), has investigated the range of new cybersecurity risks present in these environments, and I discuss four of the top concerns here:

1. Security mindset

De-prioritisation of a security mindset because of heightened anxiety, stress, depression, burnout, and poor mental health generally motivated by the pandemic. As individuals concentrate more on basic needs (e.g., safety, health, family, job security), they may be less cognisant of workplace security concerns; or may assume that security is purely the organisation's responsibility. This continues to be true today because there has been little mental and psychological break/downtime for many individuals since the pandemic began.

2. Security training

Lack of security training for the remote working environment resulting in poor security practices that increase the potential of a compromising cyber-attack. Many organisations were not able to train employees adequately or build a strong security culture before they were forced to work from home. Even now as they return to offices, there is a lack of general understanding about security culture and related practices (Uchendu et al., 2021).

3. Remote working insider threat

Remote workers may, in rare cases, exploit the lack of management monitoring or oversight to steal confidential information from their employer or misuse corporate services. Although not the norm, cases of insider threat by remote workers may be motivated by perceived, or actual, job insecurity due to the pandemic; a period where many have been laid off or made redundant.

4. Returning to work

After a long period of remote working, employees returning to offices may bring infected devices into the Critical National Infrastructure (CNI) and corporate networks. Home networks are much more likely to be compromised than CNI and corporate networks, and therefore the extended period of remote working can escalate this risk. This also poses a significant challenge for employers and IT teams as they try to reintegrate employees into the office environment.

These risks are novel given the context of COVID-19, and the combination of technological, social, and psychological factors that they are based upon. Cybersecurity teams need to appreciate the socio-technical nature of the risk, and plan, create and test solutions that accommodate these factors.

> **"De-prioritisation of a security mindset because of heightened anxiety, stress, depression, burnout, and poor mental health generally motivated by the pandemic."**
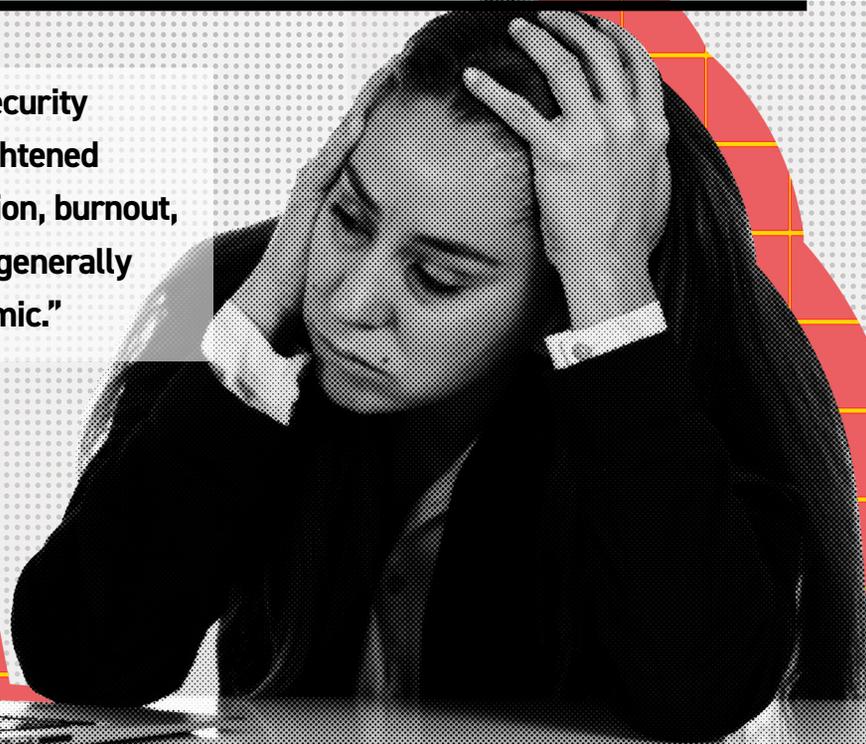
WHY IS PRIVACY IMPORTANT TO THIS DISCUSSION?

While security tools can be viewed as enablers of privacy (e.g., end-to-end encryption in communications software such as Zoom, Signal or WhatsApp), in some contexts, security and privacy are regarded as competing goals. For instance, as organisations sought to secure and manage remote workforces, there was a marked increase in the use of remote employee monitoring and surveillance tools. This led to several new widespread risks, this time to employees' privacy:

- **The potential infringement of employee's privacy caused by a dramatic surge in employer usage of (remote) workplace surveillance/monitoring technologies.** This could include monitoring of keystrokes, screens and websites visited. A significant reality is that in some cases, employees may be using their own technologies (iPads, smartphones, laptops) for remote working, thereby giving employers (or the companies they outsource security management to) access to vast amounts of personal employee data.

- **New forms of technology (e.g., smart technologies) emerging during the pandemic that can monitor employee emotional state could also violate privacy.** For example, such emotional and psychological data, if not properly protected, may be used to profile employees according to their wellbeing, and thus impact employment or future career prospects.

> "A significant reality is that in some cases, employees may be using their own technologies for remote working, thereby giving employers (or the companies they outsource security management to) access to vast amounts of personal employee data. "

Privacy is an important consideration for employers because of the need for trust between employee and employer, regardless of sector. If employees perceive that there is excessive, unwarranted monitoring, this could lessen their trust in, or commitment to, the organisation.

There is, therefore, a delicate balance to be maintained. As governments, policymakers, corporations and SMEs seek to weather the plethora of cyber-attacks that continue to emerge, developing cybersecurity solutions that also consider employee privacy concerns is paramount.

....

Dr Jason R.C. Nurse is an Associate Professor in Cyber Security at the University of Kent and a Visiting Academic at the University of Oxford. His research focuses on organisational cyber security, insider threat, and human aspects of security and privacy.

LORRAINE BOWMAN GRIEVE

COVID-19 CONSPIRACY IN IRELAND AND THE FAR-RIGHT NEXUS

Many have asked if there is a link between a rise of the far right and COVID-19 related conspiracy theories. Lorraine Bowman Grieve looks at the evidence in Ireland.

'The rise of the far right' in Ireland has been widely discussed in mainstream media, however, the extent of this 'rise' remains largely unknown. Additionally, with much uncertainty remaining about the future and the ongoing impact of COVID-19, it is perhaps unsurprising that conspiracy theory belief also appears to be on the rise in Ireland.

Is there a nexus between the two? While much has been written about the psychology of conspiracy theories and how best to measure the construct, there remains a dearth of any applied research in the Irish context.

During the global pandemic, there has been a rise in conspiracy theory production and dissemination, with many theories having an international component while also demonstrating a more localised impact. For example, the theory of a (globally) planned pandemic to facilitate (national) government control. The nature of conspiracy theories is such that once they are in the public sphere, they can be influential in various aspects of decision making, although the extent of this remains poorly measured.

LOOKING FOR ANSWERS

Since March 2020, Ireland has used 'rolling lockdowns' in attempts to lessen the impact of COVID-19. This has resulted in varying levels of frustration with pandemic related government policies, such as travel limitations, mask requirements, and vaccine rollout. In turn, this has compounded existing dissatisfaction with government policies (relating to homelessness, housing, and unemployment) and created a space for angry and disillusioned people looking for answers.

Some people are finding these answers in far-right ideologies, COVID-19 conspiracy theories, and 'scamdemic' rhetoric. What we do not yet know, and need to understand more fully, is the extent of belief in far-right ideologies in Ireland. This will allow us to examine the nature of the relationships between these beliefs and COVID-19 conspiracy creation and dissemination and understand the potential impact on behaviour.

To date, despite Ireland having some conditions which may seem conducive to the growth of the far right (such as economic change, fluctuating employment levels, a housing crisis, and continued emigration and immigration), it has remained the less popular option.

The results of the 2020 General Election demonstrated how little palate the Irish voting public have for a right-wing nationalist party. Neither the National Party nor the Irish Freedom Party (both considered far-right in terms of ideology) has representation at a local or national level and, between them, received less than 1% of the vote in the 2020 election. This could be because Sinn Féin has increased in popularity and provides the alternative people seek in the Irish context.

THE FAR RIGHT AND COVID-19 CONSPIRACY

However, as Sinn Féin has become more mainstream, this may provide the necessary 'space' for the far right to begin to flourish.

The Virus is **GLOBALISM**

The Antidote is **NATIONALISM**

NP AN PÁIRTÍ NÁISIÚNTA THE NATIONAL PARTY nationalparty.ie/join

Globalism vs Nationalism, 2020 | Flickr.com

National Party members at the March for Innocence, 2020 | Flickr.com

To this end, there are vocal proponents of right-wing ideology within the Irish context, and interestingly these individuals are now often linked with the dissemination of COVID-19 conspiracy theories. Currently, we find intertwined discourses created around anti-lockdown restrictions, anti-mask and anti-vaccination campaigns, as well as anti-immigration views more broadly.

> **As Sinn Féin has become more mainstream, this may provide the necessary 'space' for the far right to begin to flourish.**

Increased online monitoring by Moonshot (following the events at Capitol Hill in January 2021) has led to some shifts in online media use by far-right proponents in Ireland. For example, according to Gallagher and O'Connor (2021), Telegram has become one of the main communication tools for Irish far-right groups, influencers, and supporters. Their analysis illustrates that the far-right is intersecting with Irish anti-lockdown and COVID-19 conspiracy theory Telegram channels, actively encouraging followers to spread disinformation.

Realistically, in Ireland as elsewhere, more data are needed to provide a clear picture of how the far right interacts with COVID-19 conspiracy theories (and indeed the far left). There are inherent challenges in gauging the popularity of an ideology within a population. However, much of what we assume to know about 'the rise of the far right' in Ireland is based on media speculation and a limited number of empirical studies.

As the COVID-19 pandemic does not seem to be ending any time soon, there is an urgent need for in-depth studies of these communities, their messaging, and the evolving channels they communicate through. Comparison of in- and between-country change will also help understand and disrupt two global challenges, with significant national impacts.

....

Dr Lorraine Bowman Grieve is a Lecturer in Psychology at Waterford Institute of Technology, Ireland. She is primarily interested in the application of social psychology to understanding behaviour and phenomena related to terrorism, counter-terrorism, and the range of ethical issues related to such research. She has published research on the conceptualisation of cyberterrorism, understanding anti-abortion extremism, Irish republicanism online, and right-wing extremism.

ANDREW SILKE, JOHN MORRISON, HEIDI MAIBERG, CHLOE SLAY & REBECCA STEWART

THE PHOENIX MODEL:
DISENGAGEMENT AND DERADICALISATION

Derived from a systematic review of contemporary research, a new model for understanding disengagement and deradicalisation processes has been produced. The team behind the Phoenix Model takes us through its development.

MODEL SYNOPSIS

In a review of disengagement and deradicalisation literature from 2017 to 2020, we identified 11 major themes: Opportunity, Disillusionment, (Dis)trust, Family and friends, Prison, Identity, Programme interventions, Formers, Security, Mental health, and Reintegration.

Many of these themes have been flagged as significant factors in disengagement and deradicalisation before, though this is the first time they've been identified as a collective and this systematic approach allowed further analysis to suggest a new model for understanding disengagement and deradicalisation processes.

Within these themes, we identified three catalysts: actor, psychological, and environmental, that play interconnected roles in an individual's disengagement and/or deradicalisation. The themes relating to each catalyst category are as follows:

CATALYSTS

- **Actor catalysts:** Family and friends, Programme interventions, Formers
- **Psychological catalysts:** Disillusionment, Mental health
- **Environmental catalyst:** Prison

In our review, prison was the only environmental catalyst we identified. However, with further assessment, a wider variety of environmental catalysts may also be identified.

FILTERS

The catalysts' impact can either be positively or negatively affected by a series of filters:

- [Dis]trust
- Perceived opportunity
- Security

These filters play the role of refining which individual will successfully go through the disengagement/deradicalisation processes. The filtering variable of (dis)trust is critical regarding the actor catalyst(s). If the individuals promoting or supporting disengagement/deradicalisation are trusted, this leads to a greater likelihood of a positive outcome. In contrast, if distrusted, this can lessen the possibility of successful disengagement/deradicalisation.

Even with the positive impact of actor, psychological, or environmental catalysts, an individual will not be likely to disengage/deradicalise unless they are provided with a credible, positive, and sustained opportunity. However, even with the presence of this perceived opportunity, if there are significant and credible security concerns for the individual, then the process leading to successful reintegration may be impeded. This could, for example, be a threat of violence, or a perceived threat of violence, towards the disengaging individual and their family from members or allies of the group they are considering leaving.

The studies we reviewed demonstrated that the individual is going through a gradual identity transformation throughout the whole process – a central aspect of the Phoenix Model. The role of identity across the studies varied on an individual basis and with different issues flagged, including:

1. The rejection of an existing extremist identity
2. The search and elevation of an alternative identity
3. The transformation of a militant identity into a peaceful identity, embracing many similar values.

The Phoenix Model posits a central role for identity transformation in the process of change. The significance of other factors is related to how they can:

a) catalyse such change,

b) provide opportunities for it to occur, or

c) present blockages to its progress.

The diagram shows a phoenix with labeled wing feathers:

ACTOR CATALYSTS
- Programme Interventions
- Family & Friends
- Formers

PSYCHOLOGICAL CATALYSTS
- Disillusionment
- Mental Health

ENVIRONMENT CATALYSTS
- Prison

(DIS)TRUST

PERCEIVED OPPORTUNITY

SECURITY

REINTEGRATION

IDENTITY TRANSFORMATION
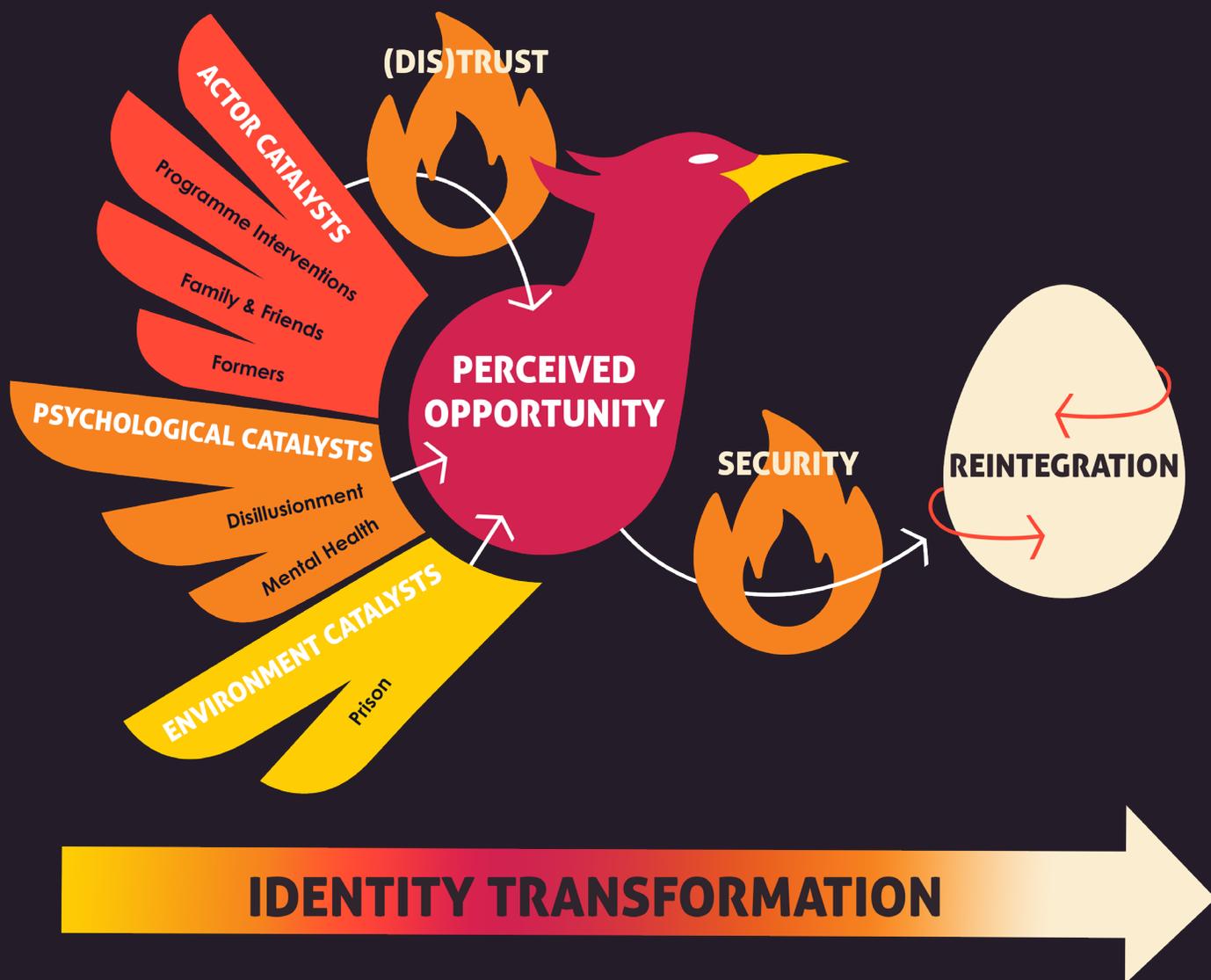
THE PHOENIX MODEL

The model was named the Phoenix Model as identity transformation (particularly in terms of the rebirth of pre-existing elements of identity) provides the foundation of the disengagement and deradicalisation processes. These pre-existing elements of identity had been subsumed or dominated by elements supportive of or embedded within the individual's life as a terrorist or violent extremist. One of the key findings of our review was that the re-emergence of the alternative identities (due to a variety of potential causes) appears to be a fundamental factor in the process of change.

In mythology, the phoenix is frequently a symbol of rebirth and renewal from the ashes of an old life. Such symbolism seemed especially apt for this new model, centred as it is on the concept of identity transformation, where the re-emergence of often old, subsumed identity elements (or the creation of an entirely new identity) provides the foundation for a move away from life as an active terrorist or violent extremist.

As highlighted in the model, such transformation can be facilitated by a range of catalyst factors that successfully pass through the identified filters; these sometimes work together and sometimes work in isolation. The evidence suggests that these processes are usually common in the lives of most terrorists and extremists. Disengagement or deradicalisation, however, is not necessarily inevitable.

It is worth noting that the model reflects the significant findings from recent research in this area, but we are not arguing that other factors do not play a role in these processes. It is likely that other factors currently lack good evidence and data but will later be identified as playing a role. Yet, the strength of this new model is that it is solely derived from a systematic review of the strongest contemporary research.

Future research may highlight other relevant factors, which will lead to the significant refinement of our understanding of the role of the factors already identified and incorporated here. For now, however, we have found that these are the factors with the most robust empirical support.

INSIGHTS

The Phoenix Model offers a range of potential insights and applications in terms of policy and practice. At a fundamental level, it highlights factors found to facilitate the disengagement and deradicalisation processes. The model also suggests how these factors can interact and flags issues that should be considered when designing or assessing the impact of initiatives in this area.

Overall, the model argues for a key role for identity dynamics and that this can be a critical factor in disengagement and deradicalisation processes. Importantly, the nature of these dynamics and outcomes varies on an individual basis. The research suggests that it is crucial to consider identity – and what happens to it – when considering the design and evaluation of interventions in this field.

The model also supports the development and use of disengagement and deradicalisation programmes with terrorist and extremist offenders. The systematic review found that these interventions generally show positive impacts in a majority of cases. However, they do not 'work' in 100% of cases, and evidence is currently lacking on what elements of such programmes are the most effective. This needs to be a priority for future research.

NEXT STEPS

While there is much to be encouraged about in considering the Phoenix Model, caveats remain. In particular, the quality of the research data in this area (though notably improved in recent years) still lags behind the standards common in many other areas, such as our understanding of desistance processes with non-terrorist offenders.

Though a large number of studies were initially identified as relevant, ultimately, very few made the quality benchmark criteria we set. Even among these studies, with a few exceptions, we note that the majority relied on qualitative methodological approaches such as semi-structured interviews, autobiographical analysis, and case study analysis. With one notable exception, research rarely made use of comparison or control groups.

We are not arguing that these research methodologies are not valuable, on the contrary. However, for our understanding of disengagement and deradicalisation to continue developing, there needs to be greater variety and sophistication in our methodological and analytical approaches. Addressing such concerns is one area that requires significant attention in future research.
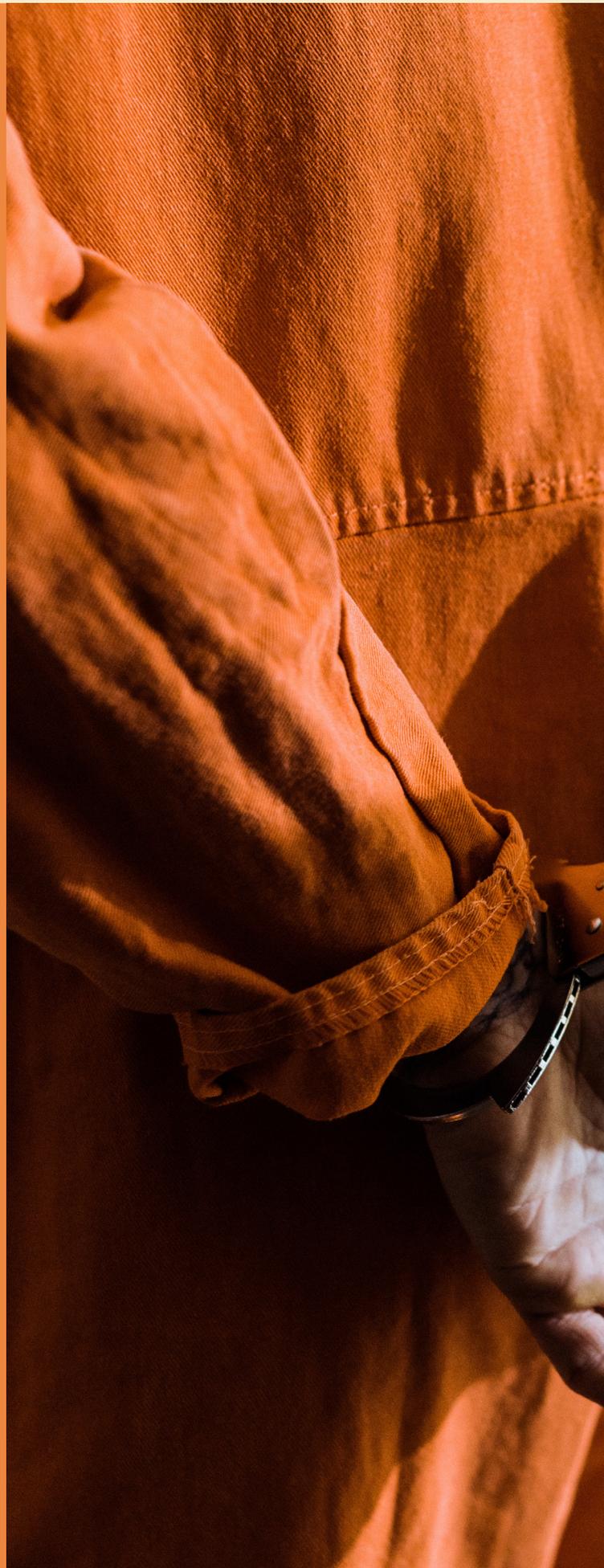
> **The strength of this new model is that it is solely derived from a systematic review of the strongest contemporary research.**

There are several important subjects on which data are currently lacking. For example, there is limited information available on the timing of disengagement and deradicalisation processes. Some research presents the length of time this process can take, however, we need more in-depth knowledge about this timing. It would greatly benefit those designing disengagement and deradicalisation programmes to have an understanding as to whether there are, for example, significant transition periods or windows for supporting change.

Further, though the initial evidence in this area is encouraging, more independent assessments are needed of the impact of programmes designed to facilitate disengagement or deradicalisation. Such programmes frequently come in for harsh public scrutiny around their effectiveness. The available evidence, however, is generally limited and often of patchy quality. In particular, the current state of knowledge is very poor at identifying what elements of the different programmes have the most impact. As most interventions comprise multiple elements, this creates uncertainty over what works best overall, and there remains a pressing need for robust evaluations of these interventions.

Another critical issue that needs more attention is the risk of backsliding. Current research does not provide much insight into the processes and risks around apparently disengaged or deradicalised individuals later reengaging with terrorism. Relapse and recidivism occur but appears to be uncommon. A growing body of research suggests that recidivism rates for terrorist offenders, for example, are comparatively low. However, a more systematic understanding of the factors involved in backsliding is clearly needed.

An empirically led understanding of why and how individuals reengage with terrorism would allow practitioners to develop more resistant support structures to assist in developing a more sustainable disengagement process.

Andrew Silke is Professor of Terrorism, Risk & Resilience at Cranfield University.

John Morrison is a Senior Lecturer in Criminology at Royal Holloway, University of London.

Heidi Maiberg is a PhD Candidate at Royal Holloway.

Chloe Slay and Rebecca Stewart are graduates of the MSc in Terrorism and Counter-Terrorism Studies at Royal Holloway.

Image credit | LightField Studios / Shutterstock.com

SIMON COPELAND

ISLAMIC STATE, FILTERS, AND PHOTOSHOP

How the Islamic State edits its images to support its narratives.

The carefully curated aesthetic of the Islamic State's (IS) visual media has helped its 'brand' achieve global recognition. However, its skilful editing of photographs also serves another purpose; to subtly shape how its outputs are 'read' and reinforce the narratives it wishes to advance.

Whilst images have traditionally received less attention than text in studies of extremist propaganda, the visual-heavy media outputs of contemporary terror groups – in particular, al-Qaeda and IS' digital magazines – have brought about new interest in this area. This work demonstrates how jihadi groups use images of particular symbols with cultural or theological significance such as lions (a motif of bravery, strength and valour in Islamic art and culture) to add weight to their narratives. This content-focused approach, however, fails to address how the 'slick' and 'glossy' visuals in these publications appeal to and inspire an audience who have grown up in a world of 'Instagram aesthetics' and photo-editing software on their phones.

Virtually every photograph within IS' English-language magazines (Dabiq and Rumiyah), even those that depict relatively mundane content, display signs of extensive editing with programmes such as Photoshop or Lightroom. Included are adjustments to colour, contrast, light and dark balance and the digital addition of photographic techniques or effects such as lens flare – or a phenomenon where bright light enters a camera and scatters, resulting in a haze or starburst. These amendments influence the stories that these images tell, even if only subtly – something IS looks to exploit to ensure that the photographs in its magazines reinforce the narratives contained within the text.

IS' use of stereotypical 'Western' social media aesthetics is often acknowledged but little explored outside of a branding context. Synonymous with Instagram, digital filters mimic those

X-Pro II   Nashville   Inkwell

added to camera lenses to give photographs a distinct 'look' by modifying the balance of contrast, sharpness and the intensity, saturation and luminosity of certain colours. The flat, muted tones and limited colour palettes that characterise the pictures in IS' magazines can be quickly and easily applied to new images through pre-saved filters. The reds of blood and gruesome injuries are also commonly made more vivid in these publications in an effort to elicit different emotional reactions depending on whether IS deems the subjects as innocent victims or deserving of such violence.

Elsewhere, colour is manipulated in Dabiq and Rumiyah in other, much more subtle ways. Images of Western cities are often edited in line with Instagram trends for 'moody' urban and street photography – long exposures and contrasting neon colours of lights contrasting with dark shadows painting particularly garish portraits of these decadent, immoral and corrupt societies. However, images accompanying articles urging individuals to travel from the West to Syria and Iraq flip this colour palette on its head; the cityscapes becoming highly desaturated, grey and bleak in contrast to golden, sunlight-illuminated planes that symbolise making this journey.

Photographs of the coffins of US troops are given similar treatment. Images are desaturated to emphasise the unwinnable grind that America's contemporary military engagements have come to represent. IS' enemies are given a sallow, sinister appearance, their pupils reduced to solid black, and they resemble demons or monsters.

Another photo-editing technique, synonymous with Photoshop and Instagram, that is frequently used within Dabiq and Rumiyah is vignetting – or the reduction of an image's brightness around the periphery, compared to the centre. One issue of Dabiq features an image of former Iranian President, Mahmoud Ahmadinejad, and

a rabbi engaged in close dialogue; the dark vignette framing the two men only serving to emphasise the closeness between them. Such editing serves to paint IS' enemies or 'disbelievers' as being steeped in darkness or ignorance and supports narratives that these duplicitous enemies of Islam are conspiring in the shadows to bring about its downfall. In this sense, images help cultivate an aesthetic not only for IS itself but also for its enemies.

Like darkness, light is also central to IS imagery. Sun-drenched pictures of fighters, citizens and locations under its control dominate the visual landscape of Dabiq and Rumiyah. Whilst this light has often been captured by the original photographer, images are frequently digitally manipulated to add or increase the appearance and intensity of sunshine falling on fighters, civilians and locations that make up IS' caliphate.

Unsurprisingly, such edits advance narratives that the subjects are righteous, blessed or otherwise on the path to salvation. Lens flares are also commonly added to images of guns to give the effect that the sun shines out from the barrel; something that supports narratives that a glorious future or paradise will only be achieved through violence.

Assumptions that photographs capture events 'as they happened', or are neutral, value-free and evidential rather than carefully curated, make them a powerful resource for extremist groups to deploy in their propaganda. Interrogating the 'texture and technique' of the Islamic State's photography editing reveals the subtle ways in which images are manipulated to become an extension of the narratives advanced in the text in its English-

> "Virtually every photograph within IS' English-language magazines (Dabiq and Rumiyah), even those that depict relatively mundane content, displays signs of extensive editing."

language magazines. Other militant groups have already looked to step up their propaganda in response to IS' comprehensive media strategy, including its 'slick' aesthetic.

Therefore, understanding and attempting to counter the appeal of extremist media requires further appreciation and interrogation of the sophisticated photo-editing techniques these groups use to enhance how text and images intersect at various levels to provide engrossing narratives. Highlighting how certain images have been deliberately manipulated may, however, provide practitioners with opportunities to challenge the authenticity of extremist narratives and the credibility of their authors.

Dr Simon Copeland is a Postdoctoral Researcher at Swansea University's Cyber Threats Research Centre (CyTREC). His work focuses on extremist networks, propaganda and narratives.

ANNA LESLIE

THE ELICITING INFORMATION FRAMEWORK

A VEHICLE FOR RESEARCH INTO PRACTICE

Anna Leslie talks about the Eliciting Information Framework she designed to assist practitioners in navigating the existing evidence base and more successfully applying it to their work.

There is a wealth of behavioural and social science research that is relevant to the work of practitioners such as source handlers, police interviewers and negotiators. CREST has published over 100 articles directly relating to interviewing alone. Much of CREST's other research streams, such as understanding beliefs and ideology, are also relevant to those interviewing suspected terrorists or handling sources who are providing intelligence on terrorist groups. Members of the police and intelligence agencies, alongside academic researchers, have been involved in using such research to train and advise their frontline colleagues for years.

However, there have been problems with the application of the science to practitioners when they are out doing their jobs. Some training sticks well, but some does not. Some behavioural science techniques are easy to apply, others take time and a lot of guidance. In addition, the wealth of available information can even be a blocker to engaging with behavioural science advice. Practitioners do not always know where to start, or how different approaches may support or contradict each other.

In 2016, CREST held a Masterclass in Eliciting Intelligence event for over 50 practitioners. One of the questions asked of the panel was what advice they had on when to use which technique. The panel agreed that this was the next step for the research community, determining which techniques are the most effective with which sort of interviewees and in what sort of context.

> **We also add value not only by discovering something new but also by packaging it up in a digestible way.**

Whilst that research is essential (especially in the context of agent handling, which is different from police interviewing), we also add value not only by discovering something new but also by packaging it up in a digestible way (Taylor, 2016).

Part of my role as one of CREST's Research to Practice Fellows is to develop innovative ways to encourage the application of science to our stakeholder's day jobs. Discussions with our stakeholders a few years ago echoed the question asked in the CREST Masterclass, they wanted:
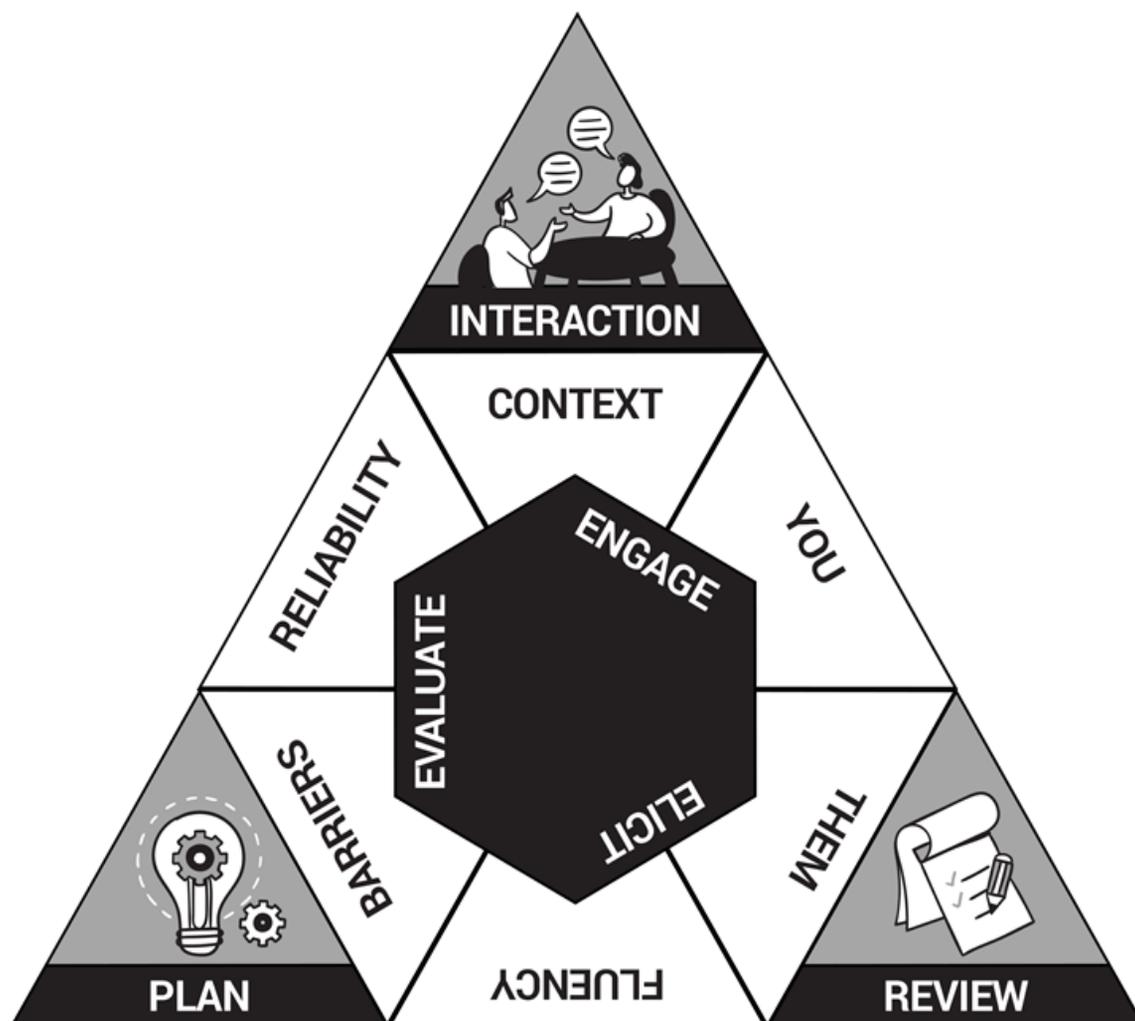
- Clear advice on when particular techniques should be used.

- Help in bridging the disconnect between the relevant research and the specific issues they were facing with a case.

- To understand how to pull together techniques and research to produce coherent training courses.

THE FRAMEWORK

To help with these problems, I designed the Eliciting Information Framework based on a clustering process of existing training material, tools, techniques and research as well as an understanding of the process and decision making that practitioners engage in when interviewing or debriefing others.

This work builds on existing frameworks, such as that published by Brandon, Wells & Seale (2018), but is more flexible in its application. Brandon et al's science-based approach to interrogations details specific techniques that should be used at different stages of an interrogation, whereas the Eliciting Information Framework groups those techniques together to form categories. This allows for the practitioner to select the most appropriate technique for their needs

> **The Eliciting Information Framework is applicable to all practitioners whose role is to elicit information, negotiate, or build relationships with others.**

and also allows the framework to be updated with new research as it become available.

The Eliciting Information Framework is applicable to all practitioners whose role is to elicit information, negotiate, or build relationships with others, whether in a debrief, a more formal interview, or a conversation. It is designed to assist practitioners to better navigate the existing research. It aims to enable them to apply the research more easily to their work, ensuring maximum yield of information and successful relationship maintenance.

PHASES

PLAN

INTERACTION

REVIEW

INTERACTION
CONTEXT
RELIABILITY
YOU
ENGAGE
EVALUATE
BARRIERS
ELICIT
THEM
PLAN
FLUENCY
REVIEW

PROBLEM SPACES

CONTEXT
RELIABILITY
YOU
BARRIERS
THEM
FLUENCY

FUNCTIONS

ENGAGE
EVALUATE
ELICIT
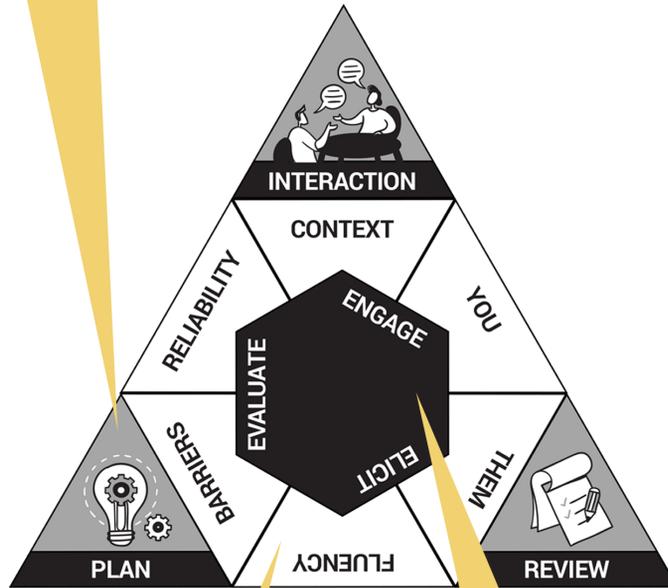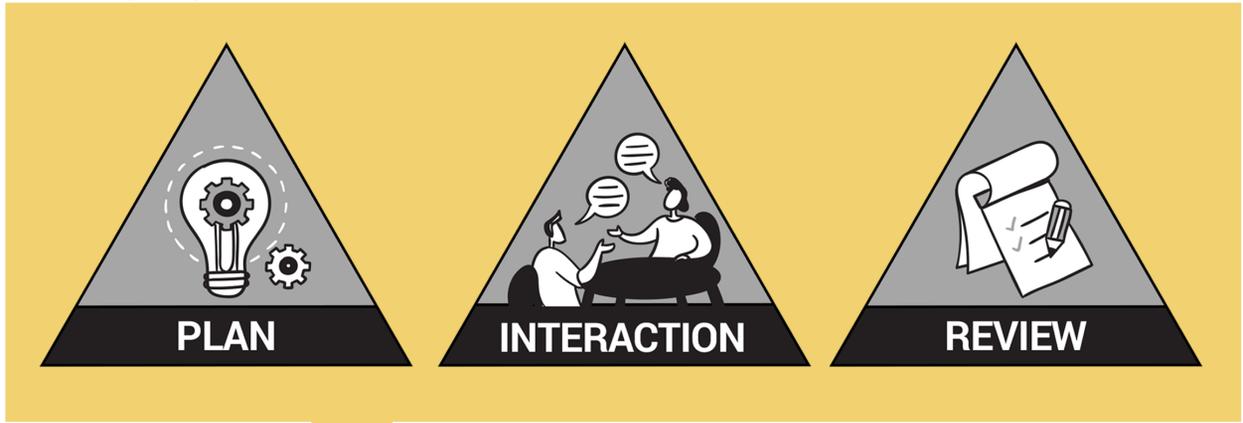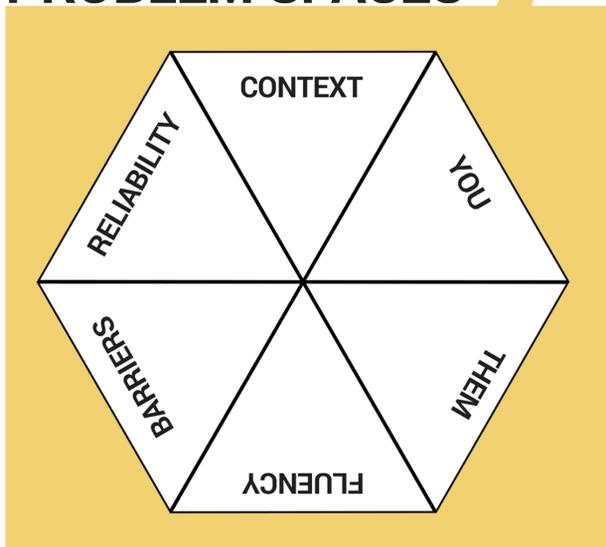
It is also a practical tool, designed to give structure to the planning, execution and reviewing phases of an interaction for those leading them and those that offer advice, guidance and training. It provides all practitioners with a shared, evidence-based, mental model and a shared language so they can think as a team to identify potential problems more easily and to reach meaningful solutions aided by behavioural science techniques.

The framework has three core components:

1. Phases
2. Functions
3. Problem spaces

1. THE PHASES

The phases (**PLAN, INTERACTION, REVIEW**) are equally as important and should be carried out during every application, but they will vary in the amount of time they take. They are also cyclical, so the decisions made in the REVIEW phase will feed into the PLAN phase next time.

2. THE FUNCTIONS

The functions are what practitioners should be focusing on and thinking about during each phase of the process. These are:

- **EVALUATE** (monitor in the moment what is happening),

- **ENGAGE** (build a positive relationship with your contact),

- **ELICIT** (gain as much credible information as possible).

3. THE PROBLEM SPACES

The six problem spaces are areas that practitioners can explore/ seek to understand if they have particular issues with their case. These are not exclusive (there is a necessary overlap between them all) but they are exhaustive (there should not be issues that do not fit within these categories).

The problem spaces are **CONTEXT, YOU, THEM, FLUENCY, BARRIERS** and **RELIABILITY.**

The benefits of the framework are that it is easy to remember and replicate. It can be used during an interview, debrief or negotiation, as well as when working on a case with others. Behavioural and social science tools and techniques can be

mapped onto the framework to assist practitioners with their development (i.e., learning new skills) and problem solving on particular cases.

For example, all 'planning' tools, which help formulate an engagement strategy, can be grouped together. Or, if there is a particular issue with (for example) assessing the credibility of an interview after it has taken place, then tools that are mapped with REVIEW, ELICIT, RELIABILITY may be useful to try.

The framework can be taught early on in someone's career and continue to be built upon. The shared mental model and shared language should aid decision making and advice delivery.

EVIDENCE BASE

Due to a lack of field validation, it is not always possible to use techniques that are well developed from a scientific perspective in the particular context that many of our stakeholders work in.

However, just because techniques are validated in different contexts, or have only been tested in a handful of experiments, does not render them useless. On occasion, practitioners may need to use techniques derived from a limited evidence base and our use of bookstack icons (below) offer a simple way for them to assess the evidence base on which a technique is derived. These serve only as a guide but should help users make an informed decision on the potential utility of a particular technique.

In application to-date the framework has offered practitioners a useful vehicle for applying research to practice. It requires constant updating to ensure it pulls on the latest and best research, and training delivered by people with an understanding of both the problem area and the research. Early feedback has suggested the framework has the potential to play a positive and transformative role in how practitioners apply research and we continue to seek new organisations and teams to help us test and improve its delivery.

Anna Leslie is a Research to Practice Fellow for CREST. She applies behavioural and social science research to a range of law enforcement, security, and defence issues via training and consultancy.

If you are interested in hearing more about the framework then please email training@crestresearch.ac.uk

Limited evidence base

Growing evidence base

Established evidence base

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/covid19*

MICHELE GROSSMAN: HOW HAS COVID-19 CHANGED THE VIOLENT EXTREMIST LANDSCAPE?

Amarasingam, A. (2019). *The impact of conspiracy theories and how to counter them: Reviewing the literature on conspiracy theories and radicalisation to violence.* In A. Richards (ed). Jihadist Terror: New Threats, New Responses. London: I. B. Tauris/Bloomsbury, 27–40

Amarasingam, A., Argentino, M.-A. (2020). *The QAnon conspiracy theory: A security threat in the making?* CTC Sentinel 13(17), 37–44 *https://bit.ly/3AAswO3* 🔓

AVERT Research Network. (2021). Submission to Parliamentary Joint Committee on Intelligence and Security Inquiry into Extremist Movements and Radicalism in Australia. *https://bit.ly/3DEy9wF* 🔓

Banas, J. A., Miller, G. (2013). Inducing resistance to conspiracy theory propaganda: testing inoculation and metainoculation strategies. *Human Communication Research* 39(2), 184–207. *https://bit.ly/3BDjxwH*

Braddock, K. (2019). Vaccinating against hate: Using attitudinal inoculation to confer resistance to persuasion by extremist propaganda. *Terrorism and Political Violence. https://bit.ly/3FFcNkm*

CRIS (Centre for Resilient and Inclusive Societies), (2021). Submission to Parliamentary Joint Committee on Intelligence and Security Inquiry into Extremist Movements and Radicalism in Australia. *https://bit.ly/3DEy9wF* 🔓

Europol. (2021). European Union Terrorism Situation and Trend Report 2021 (TESAT). *https://bit.ly/2YJXfL9* 🔓

Federico, C. M., Williams, A. L., Vitriol, J. A. (2018). The role of system identity threat in conspiracy theory endorsement. *European Journal of Social Psychology,* 48(7), 927–328. *https://bit.ly/3AykiFZ* 🔓

GNET (Global Network on Extremism and Technology), (2020). What is QAnon? *https://bit.ly/3vdxOyo* 🔓

Khalil, L. (2020). Cross-promotion. GNET Insights. *https://bit.ly/3oVXVbF* 🔓

Khalil, L. (2021). The impact of natural disasters on violent extremism. *ASPI Counterterrorism Yearbook 2021. Canberra: Australian Strategic Policy Institute,* 107–112. *https://bit.ly/3DBeUUM* 🔓

Lowe, P. (2021). Young people and violent extremism in the COVID-19 context. *ASPI Counterterrorism Yearbook 2021. Canberra: Australian Strategic Policy Institute,* 101–106. *https://bit.ly/3lxkqS3* 🔓

Silke, A. (2020). COVID-19 and terrorism: Assessing the short- and long-term impacts. *Pool Re Solutions Report. https://bit.ly/3lzQV27* 🔓

Sprinzak, E. (1991). The process of delegitimation: towards a linkage theory of political terrorism. *Terrorism and Political Violence,* 3(1), 50–68. *https://bit.ly/3DAPHtr*

Wilson, J. (2020). *The neo-Nazi symbol posted by Pete Evans has a strange and dark history.* The Guardian. *https://bit.ly/3ofyvLD* 🔓

NATHAN SMITH & EMMA BARRETT: LESSONS FROM A RAPID RESPONSE

Chen, Q., et al. (2020). Mental health care for medical staff in China during the COVID-19 outbreak. *The Lancet Psychiatry,* 7(4), *https://bit.ly/3atQEHs* 🔓

Greenberg, N., et al. (2020). Managing mental health challenges faced by healthcare workers during COVID-19 pandemic. *BMJ,* 368. *https://bit.ly/3p1vrNL*

Knutson, A., et al. (2015). Just-in-time training: a novel approach to quality improvement education. *Neonatal Network,* 34, 6–9. *https://bit.ly/3BAFEUN* 🔓

Leach, J. (2016). Psychological factors in exceptional, extreme and torturous environments. *Extreme Physiology & Medicine,* 5, 7. *https://bit.ly/3oXXihE* 🔓

Maguire, M., Bevan, N. (2002). User requirements analysis. In IFIP World Computer Congress, TC 13 (pp. 133–148). *Springer. https://bit.ly/2X4sWOU* 🔓

Smith, N., Barrett, E. C. (2019). Psychology, extreme environments, and counter-terrorism operations. *Behavioral Sciences of Terrorism and Political Aggression,* 11, 48–72. *https://bit.ly/3BBPyW6*

Williamson, V., Murphy, D., Greenberg, N. (2020). COVID-19 and experiences of moral injury in front-line key workers. *Occupational Medicine,* 70(5), 317–319. *https://bit.ly/2YHVMVG* 🔓

Wu, H. L., et al. (2020). Facemask shortage and the novel coronavirus disease (COVID-19) outbreak: Reflections on public health measures. *EClinicalMedicine,* 100329. *https://bit.ly/3oVMBMp* 🔓

LORRAINE HOPE, ET AL: WHERE WAS I LAST WEDNESDAY?

Garry, M., et al. (2021). Contact Tracing: A Memory Task With Consequences for Public Health. *Perspectives on Psychological Science,* 16(1), 175–187. *https://bit.ly/3BD4LpM* 🔓

JORDAN NUNAN & IAN STANIER: INTELLIGENCE GATHERING DURING A PANDEMIC

Dunn, R. (2020). Adaptive leadership: leading through complexity. *International Studies in Educational Administration,* 48(1), 31–38. *https://bit.ly/3lwXq5I*

Heaton, R. (2010). We Could be Criticized! Policing and Risk Aversion. *Policing,* 5(1), 75–86. *https://bit.ly/3FFG9iJ*

Stanier, I., Nunan, J. (2021). The impact of COVID-19 on UK informant use and management, *Policing and Society,* 31(5), 512–529 *https://bit.ly/3oVJFiZ* 🔓

LIV BROWN: MULTI-AGENCY EMERGENCY RESPONSE

Brown, O., Power, N., Conchie, S. M. (2020). Immersive simulations with extreme teams. *Organizational Psychology Review,* 10(3–4), 115–135. *https://bit.ly/2W8BRy6* 🔓

Brown, O., Power, N., Conchie, S. M. (2021). Communication and coordination across event phases: A multi-team system emergency response. *Journal of Occupational and Organisational Psychology. https://bit.ly/3BwzENd* 🔓

Home Office, Emergency Response and Recovery Non statutory guidance accompanying the Civil Contingencies Act 2004. *https://bit.ly/3zoRRue* 🔓

Power, N., Boulton, L., Brown, O. (2018). *Terror attacks: how psychological research can help improve the emergency response.* The Conversation. *https://bit.ly/2WozDk6* 🔓

The Kerslake Report: An independent review into the preparedness for, and emergency response to, the Manchester Arena attack on 22nd May 2017. *https://bit.ly/3wRFgxW* 🔓

Waring, S., Moran, J.-L., Page, R. (2020). Decision-making in multiagency multiteam systems operating in extreme environments. *Journal of Occupational and Organisational Psychology,* 93, 629–653. *https://bit.ly/3rtenzp* 🔓

STEPHAN LEWANDOWSKY & MUHSIN YESILADA: THE "INFODEMIC", INOCULATION, AND INSURRECTIONS

Basol, M., et al. (2021). Towards psychological herd immunity: Cross-cultural evidence for two prebunking interventions against COVID-19 misinformation. *Big Data & Society,* 8(1). *https://bit.ly/3DztgVp* 🔓

COVID-19 Vaccine Communication Handbook. HackMD. *https://bit.ly/3ofCRCt* 🔓

Enders, A. M., et al. (2020). *The different forms of COVID-19 misinformation and their consequences.* Harvard Kennedy School Misinformation Review. *https://bit.ly/3BCXd6r* 🔓

Juanchich, M., et al. (2021). 'Are COVID-19 Conspiracies a Threat to Public Health?' Psychological Characteristics and Health Protective Behaviours of Believers' *European Journal of Social Psychology*. *https://bit.ly/3v9cnhA*

Lewandowsky, S., Yesilada, M. (2021). Inoculating against the spread of Islamophobic and radical-Islamist disinformation. *Cognitive Research: Principles and Implications*, 6(1), 57. *https://bit.ly/30VjkS9*

Loomba, S., et al. (2021). Measuring the impact of COVID-19 vaccine misinformation on vaccination intent in the UK and USA. *Nature Human Behaviour, 5*(3), 337–348. *https://bit.ly/2YEKbH2*

Wondreys, J., Mudde, C. (2020). Victims of the Pandemic? European Far-Right Parties and COVID-19. *Nationalities Papers*, 1–18. *https://bit.ly/3FEAmtM*

LAURENCE ALISON, ET AL: THE GROUND TRUTH AFTER-ACTION REVIEW TOOL

Alison, L., et al. (2020). Project ARES: Resources to support front-line workers responding to COVID-19. University of Liverpool. *https://www.liverpool.ac.uk/project-ares/*

Alison, L., Alison, E. (2020). *Rapport: The Four Ways to Read People.* Penguin Random House. *https://bit.ly/3eJjiNRz*

Mathieu, J. E., et al. (2000). The influence of shared mental models on team process and performance. *Journal of Applied Psychology*, 85(2), 273–283. *https://bit.ly/3BCmGNw*

NHS (2020). Interim People Plan 2020-2021. *https://bit.ly/30WovOT*

The Lancet (2020). COVID-19: protecting health-care workers. *Lancet, 395*(10228). *https://bit.ly/2YJlTvn*

Walton, M., Murray, E., Christian, M. D. (2020). Mental health care for medical staff and affiliated healthcare workers during the COVID-19 pandemic. *European Heart Journal: Acute Cardiovascular Care, 9*(3), 241–247. *https://bit.ly/3FQeITw*

For more information and the tool: PROJECT ARES | Ground Truth (*ground-truth.co.uk*)

JASON R.C. NURSE: BALANCING CYBERSECURITY AND PRIVACY IN THE REMOTE WORKFORCE

Lallie, H.S., et al. (2021). Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-crime and Cyber-attacks during the Pandemic. *Computers & Security*, 105, 102248 *https://bit.ly/3FCWJ2G*

Nurse, J.R.C., et al. (2021). Remote Working Pre- and Post-COVID-19: An Analysis of New Threats and Risks to Security and Privacy. In HCI International 2021 - Posters, edited by Stephanidis, C. et al., *Communications in Computer and Information Science*. *https://bit.ly/3iYbrHN*

Uchendu, B., et al. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, 109, 102387. *https://bit.ly/30TJgNV*

LORRAINE BOWMAN GRIEVE: COVID-19 CONSPIRACY IN IRELAND AND THE FAR-RIGHT NEXUS

Brotherton, R., French, C., Pickering, A. (2013). Measuring belief in conspiracy theories: the generic conspiracist beliefs scale. *Frontiers in Psychology*. 4. 279 *https://bit.ly/3mPHDy6*

Charalambous, G., Lamprianou, I. (2016). Societal Responses to the Post-2008 Economic Crisis among South European and Irish Radical Left Parties: Continuity or Change and Why? *Government and Opposition*, 51(2), 269. *https://bit.ly/3lzRI35*

Douglas, K. M. (2021). COVID-19 conspiracy theories. *Group Processes & Intergroup Relations*, 24(2), 270–275. *https://bit.ly/3FIiXAv*

Douglas, K. M., et al. (2019). Understanding conspiracy theories. *Advances in Political Psychology*, 40(1), 3–35. *https://bit.ly/3lzt9Dj*

Gallagher, A., O'Connor, C. (2021). Layer of Lies: A First Look at Irish Far-Right Activity on Telegram. *Report for Institute of Strategic Dialogue*. *https://bit.ly/3jfshST*

Gallagher, C. (2020). *The far right rises: Its growth as a political force in Ireland* The Irish Times. *https://bit.ly/3BNlVkw*

Goreis, A., Voracek, M. (2019). A Systematic Review and Meta-Analysis of Psychological Research on Conspiracy Beliefs: Field Characteristics, Measurement Instruments, and Associations With Personality Traits. *Frontiers in Psychology*, 10. *https://bit.ly/3BAxYll*

Grodzicka, E. D. (2021). Taking vaccine regret and hesitancy seriously. The role of truth, conspiracy theories, gender relations and trust in the HPV immunisation programmes in Ireland. *Journal for Cultural Research, 25*(1), 69–87. *https://bit.ly/2X9P5LU*

O'Malley, E. (2008). *Why is there no Radical Right Party in Ireland?* Working Papers in International Studies Series. *https://bit.ly/3FCtBbQ*

Pummerer, L., et al. (2021). Conspiracy Theories and Their Societal Effects During the COVID-19 Pandemic. *Social Psychological and Personality Science*, 1–11. *https://bit.ly/3DBddGE*

Shahsavari, S., et al. (2020). Conspiracy in the time of corona: automatic detection of emerging COVID-19 conspiracy theories in social media and the news. *Journal of Computational Social Science*, 3, 279–317. *https://bit.ly/2YEGq40*

ANDREW SILKE, ET AL: THE PHOENIX MODEL: DISENGAGEMENT AND DERADICALISATION

Renard, T. (2020). *Overblown: Exploring the Gap Between the Fear of Terrorist Recidivism and the Evidence*. CTC Sentinel, *https://bit.ly/3iTXQRM*

Silke, A., Morrison, J. (2020). *Re-Offending by Released Terrorist Prisoners: Separating Hype from Reality*. ICCT Policy Brief, The Hague. *https://bit.ly/3FAgdoJ*

Taylor, C., Semmelrock, T., McDermott, A. (2019). The Cost of Defection: The Consequences of Quitting Al-Shabaab. *International Journal of Conflict and Violence*, 13, a657–a657. *https://bit.ly/3BD4d3p*

SIMON COPELAND: ISLAMIC STATE, FILTERS, AND PHOTOSHOP

Frischlich L. (2021). '#Dark inspiration: Eudaimonic entertainment in extremist Instagram posts', *New Media & Society*, 23:3, 554-577. *https://bit.ly/3awyBRa*

Glazzard, A. (2017). *Losing the Plot: Narrative, Counter-Narrative and Violent Extremism*. International Centre for Counter-Terrorism Research Paper. Available at: *https://bit.ly/3AAyTAQ*

Kendall, E. (2016). 'Al-Qa'ida And Islamic State In Yemen: A Battle For Local Audiences', in Staffell, S. and A. Awan (eds.) *Jihadism Transformed: Al-Qaeda and Islamic State's Global Battle of Ideas*, London: Hurst. *https://bit.ly/3mQvQjo*

Macdonald, S., Lorenzo-Dus, N. (2019). Visual Jihad: Constructing the "Good Muslim" in Online Jihadist Magazines, *Studies in Conflict & Terrorism*, 44(5), 363–386. *https://bit.ly/3mGeBB6*

Ruston, S., J. Halverson, (2014). 'Counter' or "Alternative": Contesting Video Narratives of Violent Islamist Extremism', in *Visual Propaganda and Extremism in the Online Environment*, edited by Carol K. Winkler and C. Dauber, 105–134. *https://bit.ly/3v3K3Nw*

Watkin, A. L., Looney, S. (2019). "The Lions of Tomorrow": A News Value Analysis of Child Images in Jihadi Magazines. *Studies in Conflict & Terrorism*, 42(1–2), 120–140. *http://bit.ly/2YkIHwS*

ANNA LESLIE: THE ELICITING INFORMATION FRAMEWORK: A VEHICLE FOR RESEARCH INTO PRACTICE

Brandon, S., Wells, S. (2019) *Science-Based Interviewing.* Bookbaby ISBN: 9781543973440

Brandon, S. E., Wells, S., Seale, C. (2018). Science-based interviewing: Information elicitation. *Journal of Investigative Psychology and Offender Profiling*, 15(2), 133–148. *https://bit.ly/30WnPfh*

Taylor, P. (2016). The promise of social science. *Crest Security Review*, issue 1, *https://bit.ly/3mGdBwQ*

CENTRE FOR RESEARCH AND
EVIDENCE ON SECURITY THREATS

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

THE CENTRE FOR RESEARCH AND EVIDENCE ON SECURITY THREATS

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

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

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

Professor Stacey Conchie, CREST Director

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