SUMMER 2021 / ISSUE 11

CREST SECURITY REVIEW

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

Risk

WHAT ARE THE BARRIERS TO AND INCENTIVES FOR ADOPTING PROTECTIVE SECURITY? – p10

TERRORISM RISK ASSESSMENT: WHAT MAKES A 'GOOD' RISK ASSESSOR? – p14

DOES A STRONG CONSPIRACY MENTALITY LEAD TO VIOLENT EXTREMIST INTENTIONS? – p20

CONTENTS

Highlights

COMMUNICATING EFFECTIVELY WITH THE PUBLIC ABOUT TERRORISM IN CROWDED PLACES

Research on the effectiveness of existing campaigns (e.g. 'See it, Say it, Sorted') in preventing attacks by increasing reporting behaviours – p8

VIOLENT EXTREMISM: THE ASSESSMENT AND MANAGEMENT OF RISK

Eight recommendations for why and how practitioners should use developments in the risk and threat assessment field – p16

RISK

CREST SECURITY REVIEW
Editor - Rebecca Stevens
Guest Editors – Matthew Francis & Paul Grasby
Illustrator & designer – Rebecca Stevens

To contact *CREST Security Review* please email
csr@crestresearch.ac.uk

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

FROM THE EDITOR

In this issue of *CREST Security Review* we highlight some of the latest research on risk; predominantly drawing attention to the challenges, and potential solutions, to assessing and managing the risk of violent extremism.

If you're new to this research and don't know your static from your dynamic risk factors, Monica Lloyd has provided a helpful A–Z guide (page 36) to the key terms found throughout this issue.

To date, the violent extremism literature has focused mainly on the search to identify the risk factors thought to have the most bearing on an individual's decision to perpetrate an act of ideologically motivated violence. Caroline Logan writes about the need for the field to evolve from this essential but limiting baseline, providing eight recommendations for improving and managing risk (page 16).

We have two articles in this issue covering the risks of terrorism in crowded places. On page 8, Brooke Rogers, Julia Pearce, David Parker, and Lasse Lindekilde discuss the effectiveness of public communication campaigns, such as 'See It, Say It, Sorted' in promoting protective behaviours. On page 10, David McIlhatton and Rachel Monaghan highlight both the barriers and incentives for protecting these publicly accessible locations.

From risk assessment to the risk assessors, Nadine Salman and Paul Gill reveal what makes a good risk assessor – by asking those making the judgements. Little is known about the practitioner's perspective on risk assessment and what they think is vital to the role, and their pilot study suggests some interesting and useful implications (page 14).

Many have noted the convergence between belief in conspiracy theories and ideological extremes. So, what is the risk of violent extremism in someone with a strong conspiracy mentality? On page 20, Bettina Rottweiler and Paul Gill's latest research investigates this relationship in detail.

In 'If this then…what? Security and privacy in trigger-action system' (page 22) Emily Collins, Phillip Morgan, and Dylan Jones look at how people can be primed to think about security and privacy when setting trigger-action rules for smart home devices. And on page 4, Steven Watson explains why a focus on risk is ineffective in changing online privacy behaviour, and how the lessons learned here can be applied to other security contexts.

Outside of this issue's focus on risk, Ian Stanier and Jordan Nunan provide a mnemonic-driven framework to help identify and understand informants' motivations (page 24); far-right narratives vary according to the beliefs of those telling them but they often reflect common themes, as a short primer by Ben Lee explains on page 28; Simon Oleszkiewicz discusses adaptive behaviour (page 32), explaining how it can be measured and how we determine its effectiveness, and Nathan Smith provides new insights that may help promote resilience in demanding environments (page 30).

You can find all the research that underpins these articles and some further reading in the 'Read More' section on page 38. 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*

STEVEN WATSON

RISK, BENEFITS, AND THE AFFECT HEURISTIC IN SECURITY BEHAVIOURS

Most of us like to think of ourselves as honest and law-abiding. Yet, the prevalence of online piracy (or, more formally, unlawful file-sharing) shows that many of us are perfectly willing to act contrary to the law.

My colleagues and I reviewed the extant literature on the determinants and consequences of unlawful file-sharing to understand why so many people were willing to break the law in this way. We found a diversity of reasons. These included people's desire for new content, personal attitudes toward and moral arguments about unlawful file-sharing, and their beliefs about social and cultural norms regarding the acceptability of unlawful file-sharing.

For a long time, the predominant approach of legislators and industry had been to try to reduce unlawful file-sharing by attempting to increase the perception of how legally risky this behaviour was, for example, through lawsuits or the introduction of punitive legislation. This focus on risk proved to be ineffectual. There are lessons to be learned regarding why this focus on risk was not effective in changing unlawful file-sharing behaviour, which transfers to numerous security contexts.

Risk is at the heart of many attempts to understand security-related behaviours and attempts to try to enact behaviour change to adhere to better security behaviours. The rather sensible underlying logic is that if people understand why their behaviour could undermine their own or others' security, they are less likely to do it. Thus, educating people about the risks associated with their behaviour, or increasing perceptions of how risky their behaviour is, should lead to people adopting more secure behaviours.

> “It was not legal threats that began to reduce the unlawful file sharing of music, but the availability and affordability of Spotify and iTunes.

However, there are reasons to be cautious here. Sometimes we engage in behaviours because of the perceived benefits they bring, and we do not necessarily think too much about potential negative consequences. This was one of the key findings of my colleagues and I when investigating why people unlawfully download copyrighted files. They do not think of the associated legal risks when engaging in unlawful file-sharing behaviour, but rather, they think of the personal benefits of owning the downloaded files themselves.

Similar logic is likely to apply to security behaviours. For example, when selecting a new password for a website, people may know that a weak password brings risks, but at that moment, they are more concerned about their ease of access and so may recycle a weak password they use on multiple websites. If we wish to change this negative user behaviour, we need solutions that address the benefits motivating these users' poor security behaviours. After all, it was not legal threats that began to reduce the unlawful file-sharing of music, but the availability and affordability of Spotify and iTunes; legal services that met the perceived benefits of unlawful file-sharing in terms of diversity and availability of content. Therefore, if we want people to use strong passwords, they probably need a convenient, easy-to-use solution as much as they need a warning that their security behaviour is suboptimal.

There are additional challenges that come from instances where individuals are more focused on benefits than they are on risks. That is because when an individual is focussing on the perceived benefits of poor security behaviours, this can actively undermine the effectiveness of any risk-based interventions via the affect heuristic.

YOU WOULDN'T STEAL A CAR

"You Wouldn't Steal a Car" is the first sentence of a public service announcement, part of the 2000s anti-copyright infringement campaign 'Piracy. It's a crime.' It was created by the Federation Against Copyright Theft and the Motion Picture Association in cooperation with the Intellectual Property Office of Singapore.

THE AFFECT HEURISTIC

The affect heuristic refers to the observation that how risky people think something is depends on how they feel emotionally about an action and its outcome. If they feel positive about the action or its consequence, then they tend to underestimate the associated risk. Conversely, if they feel negative about an action, then they tend to overestimate the associated risks. In reality, the two need not be associated at all, and often there is a positive correlation; great rewards often follow great risks.

This is why the affect heuristic is useful. It motivates us to ignore risk for beneficial outcomes or disincline taking even small risks for scant benefit. For example, this is a reason why we fall for email frauds. If an online fraudster offers us something we value greatly (such as money or the promise of romance), we tend to overlook the warning signs that offers may not be genuine.

TWO SYSTEMS OF THOUGHT

The affect heuristic is an example of what psychologists refer to as a System 1 process. System 1 processes are fast, automatic, and effortless. They contrast with System 2 processes which refer to deliberate, effortful cognitive work to think through a problem. Not surprisingly, people prefer to avoid having to use System 2 unless they have to. 'Going with our gut' and following the affect heuristic saves us a lot of time and energy and is adequate for most day-to-day decisions. However, allowing our affective processes free reign to make high-stakes decisions is a significant gamble, especially within security settings.

AFFECT HEURISTIC IN SECURITY SETTINGS

Security professionals in a range of settings must decide whether individuals, groups, or information pose a level of risk that should be acted upon. Without structured tools to guide risk assessment, errors based on security professionals' positive or negative feelings about groups or individuals are likely.

Such biases can also be created by even a small number of well-publicised events, as is likely when considering rare but high-impact scenarios such as terrorism. Fortunately, we do know of ways to reduce reliance on affective processes when making risk judgements.

> “Allowing our affective processes free reign to make high-stakes decisions is itself a significant gamble, especially within security settings.

GETTING MORE ACCURATE JUDGEMENTS

Time pressure

Time pressure increases reliance on affective processes. This pressure is one reason having mandatory tools, such as risk assessment tools, to force System 2 thinking can be helpful. It forces time-poor professionals to think through problems and not rely on gut instinct when it may not be appropriate.

Perceived anonymity

Perceived anonymity also increases affective thinking because the decision-maker assumes consequences of errors are unlikely to be traced back to them. Anonymity, therefore, lowers the risk to the individual and may reduce the requirement to engage effortfully with the risk assessment process.

Trust

When we trust organisations or groups, we also tend to perceive lower risk and rely on the affect heuristic. It is, therefore, important that trust is not misplaced.

Prevention strategies

A focus on prevention strategies (prioritising identifying as many risks as possible, even if this means some identified risks are not real) over promotion strategies (prioritising identifying only real risks) discourages affective processing of judgements. This is often appropriate in risk-averse security settings.

Presentation of information

People respond to changes in how information is presented. If the benefits of a course of action are emphasised, then the risks are assumed to be lesser. If the risks are emphasised, then the risks are believed to be greater. This means the affect heuristic can be exploited to enhance accuracy if the motives that underpin the behaviour are known.

Therefore, it is crucial to understand whether a behaviour is 1) primarily performed in order to reduce risk (high-risk salience) or 2) to gain a particular benefit (high-benefit salience). Risk salient behaviours should be promoted by reinforcing the level of risk, whereas benefit salient behaviours should be targeted by addressing the identified benefits.

For example, highlighting the dangers of not wearing a seatbelt can be effective because people only wear seatbelts because they lower risk. On the other hand, highlighting the benefits of condom use for safe sex is not always effective due to people's focus on pleasure, not risk. Hence, it would be more effective to make condoms that make sex more pleasurable. Or, returning to unlawful file-sharing, by developing legal alternatives that offer the choice and functionality of unlawful alternatives.

CONCLUSION

We know that individuals may make inaccurate judgements because of their subjective feelings, but we also know that setting up good organisational systems can mitigate these issues. Having accountable decision-making via structured risk assessment tools and providing professionals the time required to complete these correctly can lead to superior decision-making. This means more accurate risk judgements, fewer missed threats, and enhanced security for everyone.

We also know that changing poor security behaviour only through increasing perceived risk is unlikely to work in all scenarios, especially when poor security practice confers tangible benefits. We should aim to develop solutions that address these perceived benefits and make improved security as simple and pleasurable as possible.

Dr Steven Watson is an Assistant Professor in Psychology at the University of Twente. His research is in applied decision making, especially within security and legal contexts.

M. BROOKE ROGERS, JULIA M. PEARCE, DAVID PARKER & LASSE LINDEKILDE

COMMUNICATING EFFECTIVELY WITH THE PUBLIC ABOUT TERRORISM IN CROWDED PLACES

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

Effective public communication can help prevent attacks on crowded places by encouraging reporting. It can also reduce the impact of attacks that it was not possible to prevent by informing the public about how to protect themselves. Despite this, there has historically been limited research on the impact of communication campaigns on public perceptions of the likelihood or risk of terrorist attacks, or the effectiveness of the messaging in informing protective health behaviours prior to or during an attack.

Our research applies theories of risk perception, risk communication and health psychology to explore the effectiveness of existing campaigns in preventing attacks by increasing reporting behaviours (e.g. 'See it, Say it, Sorted') and protecting life by increasing the likelihood of members of the public engaging in protective health behaviours (e.g. 'Run, Hide, Tell') when an attack occurs.

SEE IT, SAY IT, SORTED

Pre-event communication is often understood in terms of providing information about protective actions that can be taken when an event occurs. Pre-event communication in a counter-terror context also has the potential to prevent a terrorist attack from taking place. We used a survey experiment to examine the impact of communication campaigns designed to encourage public vigilance and reporting on railways.

Results indicate that the 'See It. Say It. Sorted' campaign is effective in encouraging members of the public to report suspicious behaviour in train stations. However, in addition to reporting suspicious behaviour to a member of rail staff or a police officer, as requested, most respondents answered that they would also consider reporting to a member of staff in the concourse café. This highlights the importance of providing all members of staff with training on how to respond to reports, rather than only training those directly responsible for security.

Results also suggest that future public vigilance campaigns should address differences in lay and official definitions of suspicious behaviour to reduce uncertainty as a barrier to reporting, and include guidance about specific suspicious behaviours to increase reporting intentions. Specifically, our work brings further evidence to bear on previous studies indicating that members of the public tend to focus on more familiar, traditional criminal activity such as pick-pocketing or car theft. In contrast, individuals are less willing to report terrorism-related behaviours if they are uncertain about the relationship between the behaviours and attack planning. Drivers such as the perceived benefits of reporting are particularly important for increasing the likelihood of reporting suspicious behaviour on rail networks.

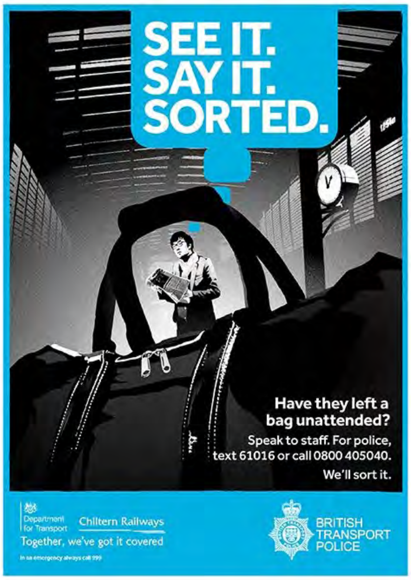
RUN, HIDE, TELL

The UK National Police Chiefs' Council released a Stay Safe film and leaflet including 'Run, Hide, Tell' guidance for members of the public in 2015 in response to marauding terrorist attacks in Paris, France. Other countries, such as Denmark, did not provide this type of pre-event communication due to concerns about scaring the public. We conducted three survey experiments, which demonstrated that 'Run, Hide, Tell' guidance does not increase perceived risk from terrorism. It does, however, increase trust by increasing public perceptions of security services' preparedness to respond and the perceived quality of police advice for keeping people safe during an attack .

Our research also found that 'Run, Hide, Tell' has a positive impact on encouraging protective behaviours (e.g. immediately running to find a hiding place) and reducing public intention to engage in risky behaviours (e.g. calling someone who may be hiding during an attack).

> "A one-year follow-up study demonstrated some reduction in positive impacts of the guidance over time."

However, it also highlights the need for future communications to address perceived response costs and target specific problem behaviours. A one-year follow-up study demonstrated some reduction in positive impacts of the guidance over time. For example, one year on, people were more likely to call someone who may be hiding during an attack than they were following


SEE IT.
SAY IT.
SORTED.
Have they left a bag unattended?
Speak to staff. For police, text 61016 or call 0800 405040.
We'll sort it.
Department for Transport
Chiltern Railways
Together, we've got it covered
In an emergency always call 999
BRITISH TRANSPORT POLICE

SEE IT.
SAY IT.
SORTED.
Are they checking security?
Speak to staff. For police, text 61016 or call 0800 405040.
We'll sort it.
Department for Transport
Chiltern Railways
Together, we've got it covered
In an emergency always call 999
BRITISH TRANSPORT POLICE

SEE IT.
SAY IT.
SORTED.
No Entry
Are they somewhere they shouldn't be?
Speak to staff. For police, text 61016 or call 0800 405040.
We'll sort it.
Department for Transport
Chiltern Railways
Together, we've got it covered
In an emergency always call 999
BRITISH TRANSPORT POLICE

initial receipt of the guidance. However, people who previously received the guidance remained more likely to adopt protective health behaviours and less likely to engage in such risky behaviour than those who had not received any information.

RUN, HIDE, TELL VS RUN, HIDE, FIGHT

'Run, Hide, Tell' remains UK official advice to the public on how to keep safe during a marauding terrorist firearms attack. However, in 2018 Norwegian security authorities issued alternative guidance to the public to 'Run, Hide, Fight'. The recommendation to 'fight' as a last resort is consistent with the US approach and informed by experience from the 2011 Utoya attack, which demonstrated that it is not always possible to avoid confrontation.

We were interested in understanding the potential benefits and unintended negative consequences of each of these campaigns. Would, for example, the UK approach discourage people from taking action as a last resort or would the Norwegian guidance encourage people to adopt risky behaviours in situations where it would still be possible to run?

Our research provides some support for both campaigns, as both sets of guidance increased public intention to adopt protective health behaviours. However, while we did not find evidence that the 'Run, Hide, Fight' campaign encouraged unwanted risky behaviours, our results did suggest that 'Run, Hide, Tell' guidance may discourage proactive planning of what to do in the worst-case scenario. This suggests that 'Run, Hide, Tell' guidance may benefit from providing additional information on what to do if it is not possible to avoid confrontation.

RECOMMENDATIONS

Our results provide evidence-based, detailed guidance about what counter-terror organisations can do to increase the likelihood of members of the public reporting suspicious behaviour, or following advice when a terrorist attack occurs.

Our work addresses practitioner concerns about causing panic or increasing fear by demonstrating that the provision of guidance does not increase the perceived risk of terrorism. It also demonstrates that communication targeted at increasing public reporting of suspicious behaviour in crowded places is effective if it reduces uncertainty and reinforces the perceived benefits of reporting. Additionally, communication designed to better enable members of the public to protect themselves if an attack occurs can enhance trust in responding organisations, as well as encouraging protective behaviours and discouraging potentially dangerous actions during a marauding terrorist attack. Unique insights include the need for communicators to:

- Provide training to all staff working in crowded places. Members of the public are likely to report suspicious behaviour to staff working in the shops and restaurants in crowded spaces, as well as security or operational staff.
- Address differences in lay and official definitions of suspicious behaviour to reduce uncertainty as a barrier to reporting.
- Include guidance about specific suspicious behaviours to increase reporting intentions.
- Communicate the benefits of reporting suspicious behaviour.
- Address the perceived response costs associated with following guidance and target specific problem behaviours.
- Provide additional information on what to do if it is not possible to avoid confrontation.

Professor M. Brooke Rogers (Professor of Behavioural Science and Security, and Deputy Head of Department), Dr Julia M. Pearce (Senior Lecturer in Social Psychology and Security Studies), and Dr David Parker (Visiting Research Fellow), work in the Department of War Studies at King's College London. Professor Lasse Lindekilde works at the Department of Political Science (Aarhus BSS) at Aarhus University.

DAVID MCILHATTON & RACHEL MONAGHAN

PROTECTING PUBLICLY ACCESSIBLE LOCATIONS FROM TERRORISM

Professors David McIlhatton and Rachel Monaghan examine some of the barriers to and incentives for the inclusion of protective security measures within the development of publicly accessible locations.

In the aftermath of the Manchester Arena suicide bomb attack of May 2017, there has been a growing demand for greater security at public spaces and venues, culminating in the call for Martyn's Law, named after Martyn Hett, who lost his life in the attack.

Martyn's Law seeks to create a clear and proportionate approach to protective security in a single piece of legislation, thereby fostering good protective security practice and clarifying responsibility for such practice, while also making sure that public bodies are prepared for terrorism so that the public is protected.

Proponents of Martyn's Law suggest it will fill the gaps in existing legislation and work more closely with cognate areas such as planning. Moreover, in February 2021, the government launched a Protect Duty Consultation, which will run until early July (Home Office, 2021). This consultation will consider how the government might utilise legislation to improve the protection of publicly accessible locations in the United Kingdom from terrorist attacks and ensure organisational preparedness of owners or operators at such locations.

The consultation is open to the public and targets those organisations, businesses etc. who own or operate at publicly accessible locations that a Protect Duty would potentially affect. As such, the consultation seeks responses to four key questions:

1. Who or where should the law apply to?
2. What should the requirements be?
3. How should compliance work?
4. How should the government best support and work with partners? (see Read More, *Home Office, 2021*).

The current counter-terrorism literature base predominantly focuses on policies and strategies concerned with preventing people from being drawn into terrorism. There is, however, a much smaller body of work concerned with protective security, essentially the defensive measures designed to counter and/or mitigate the threat and impact of terrorist attacks. Previous research (McIlhatton et al., 2019, 2020) has highlighted that enhancing the protection of publicly accessible locations from issues such as terrorism has been difficult for policymakers and practitioners.

Our research has focused on addressing this gap and examined some of the critical issues around the inclusion of protective security measures within the development of new publicly accessible locations with a specific focus on:

1. the potential barriers that may inhibit the adoption of protective security measures
2. what may incentivise the inclusion of these measures
3. recommendations for enhancing the consideration of protective security in future developments.

To address these issues, we drew on qualitative research, namely semi-structured interviews. The interviews were conducted in the United Kingdom, the United States, and Australia with over 140 professionals working in architecture, urban design, engineering (structural, civil, electrical and mechanical), planning, project management, local government representatives, real estate development and investment sectors.

POTENTIAL BARRIERS INHIBITING ADOPTION OF PROTECTIVE SECURITY

We found that key barriers were broad and not necessarily focused on issues such as cost. Some of these included:

Awareness

First, there was a lack of awareness of the terrorist threat landscape at the developer level, except where consultation with security or law enforcement professionals had taken place.

Second, there was a lack of awareness of potential design-based mitigation across the developer community, particularly for small to medium-sized developments.

> If counter-terrorism measures were to become a mainstream consideration, then they must be evident in the development brief.

Professor David McIlhatton is the Director of the Institute for Peace and Security at Coventry University and Professor of Protective Security and Resilience.

Professor Rachel Monaghan is a Professor of Peace and Conflict at Coventry University.

12

Type of client and development

Disparity existed between public and private sector developments. It was more likely that public sector clients would include security challenges, such as terrorism, within their projects. Private sector clients were less likely to stipulate such requirements unless the development related to critical infrastructure or attracted significant numbers of people at any one time. There was also a scale issue with large developers having in-house security advisors, which would enhance the likelihood that protective security measures would be considered.

Physical location of development

Some sites may not be conducive to implementing specific approaches, particularly in relation to measures such as hostile vehicle mitigation. Examples might include where site lines extend to the roadside or other infrastructure and where different ownership of land may exist.

The 'won't happen to us' mentality

Our research found a relative consensus among small to medium-sized developments, particularly those not in capital and global cities, that they were unlikely to be attacked. They didn't necessarily consider their sites to be iconic and, as such, felt that risk was low. Thus, consideration of protective security measures was likely to be limited.

Distance decay effect and impact on decision-making

The proximity of attack was expected to influence decision-making, with attacks that have occurred nearby positively influencing decision-making. This impact would decay with distance and time.

Lack of political consideration

At present, it is not mandatory to include measures related to countering and mitigating the impact of terrorism within the real estate development process, and as such, this was reducing consideration. In the UK, the proposed Protect Duty should help overcome this and mainstream the consideration of protective security across many disciplines. However, the research did find that any measures included should be proportionate to the threat and not detract from how the site was originally intended to function and its attraction for visitors and customers.

POTENTIAL INCENTIVES FOR PROTECTIVE SECURITY MEASURES

Our research highlighted that while there are barriers to overcome, there was agreement across the cohort interviewed that counter-terrorism should be a consideration in the early stages of developments. In line with this, we identified from the interviewees that there were numerous potential opportunities for incentivising their inclusion prior to formal regulation. Some of these included:

Client requirement

If counter-terrorism measures were to become a mainstream consideration, then they must be evident in the development brief. Consequently, this would involve such measures being thought about prior to writing the project requirements and training, awareness-raising, and advice should come in at this stage. In turn, attention at this early stage may reduce any retrospective challenges such as cost and design. Educating clients would be a core part of the incentivisation process.

Staff knowledge within the planning, design, and development community

Enhancing the knowledge of staff within non-cognate counter-terrorism disciplines, such as those related to real estate development –investment, planning, design, construction, costing, management – would significantly enhance the consideration of protective security measures. Many suggested that this could be done through university programs, short courses, or continuing professional development in advance of any formal regulation.

Reputational damage

The concept of reputational damage occurring because of a terrorist attack either directly or within proximity to their brand and assets, would almost certainly enhance the consideration of including protective security measures.

Understanding of threat and knowledge of resources

Many respondents, particularly those from small and medium-sized organisations and who did not have in-house security advisors, highlighted that they were unaware of the terrorist threat, other than what they saw on the news, and how the threat related to them.

Financial incentives

Numerous examples of how the government could financially incentivise protective security without regulation were discussed, including government grants for considering such measures at the earliest stage of development and tax-based incentives. These could be an important way of absorbing the upfront capital costs of introducing measures and recovering these through rebates or reductions.

Our research is broadly captured in two publications (see Read More section) and is part of a much larger research agenda focused on enhancing the scholarly knowledge base in the area of counter-terrorism and protective security, with international collaborators at the University of Ulster, the University of Central Oklahoma, and the University of Technology Sydney.

NADINE SALMAN & PAUL GILL

TERRORISM RISK ASSESSMENT: WHAT MAKES A 'GOOD' RISK ASSESSOR?

The risk assessment and management of at-risk individuals is widely used in terrorism prevention. While this relies on the judgment of practitioners, little is known about their perspective on risk assessment, and what they think is vital to the role.

We conducted a pilot study to explore this important gap in the knowledge. For this, we asked 41 professional threat and risk assessors a range of questions across three topics:

1. How, where, and by whom should terrorism risk assessments be conducted?
2. What training and experience should assessors have?
3. Which abilities and characteristics make a 'good' assessor?

The assessors surveyed came from a variety of countries and backgrounds, including law enforcement, mental health/forensic psychology, and intelligence/security. Their experience spanned from less than one year to over ten years; 44% had over ten years of experience. Sixteen assessors had direct experience using terrorism risk assessment tools, while 21 had seen or heard of them.

While the small sample size and mix of experience limit the inferences that can be made, the results nevertheless suggest some interesting and useful implications. Here is a summary of what we found, and what it means for practice.

CONDUCTING TERRORISM RISK ASSESSMENTS: WHAT, HOW, WHERE, AND WHO?

Which tools?

First, we asked the 37 assessors who had experience or knowledge of terrorism risk assessment tools about the tools they recognised, and their strengths. The most widely recognised tools were the commercially available TRAP-18 and VERA, followed by HMPPS' ERG22+. Assessors valued the ease of use and availability of the tools, as well as the usefulness of the risk and protective factors they contained.

Where?

Risk assessments can take place in person with the subject or service user, remotely (using case files and other information), or using a combination. Most assessors in the sample recommended that these assessments should be conducted in person, however, of the 16 who had direct experience in conducting terrorism risk assessments, most did so remotely. This mismatch between recommendations and practice indicates that 'best practice' may not always be possible, depending on the context.

Who?

Assessors come from a range of disciplines; panels are often multidisciplinary. Our sample recommended that risk assessments can be conducted by specialist threat or risk assessors, mental health professionals, law enforcement officers, or intelligence analysts. Most did not support the use of algorithms to replace human decision-making.

Assessors suggested that between one and ten assessors should evaluate each case. Although there was disagreement as to the exact number, most assessors favoured a panel of two or three.

ASSESSOR TRAINING AND EXPERIENCE

Formal education

The assessors in our sample recommended that terrorism risk assessors should have at least tertiary (university level) education. However, professional training and experience were considered more important.

Professional training and experience

A range of different training and professional backgrounds were suggested, with no clear consensus. Recommendations included training in specific tools or Structured Professional Judgment (SPJ) protocols, in general principles of threat and risk assessment, and in psychology or mental health. Most assessors also agreed that previous professional experience is desirable, highlighting previous psychology/clinical, law enforcement, and risk assessment experience.

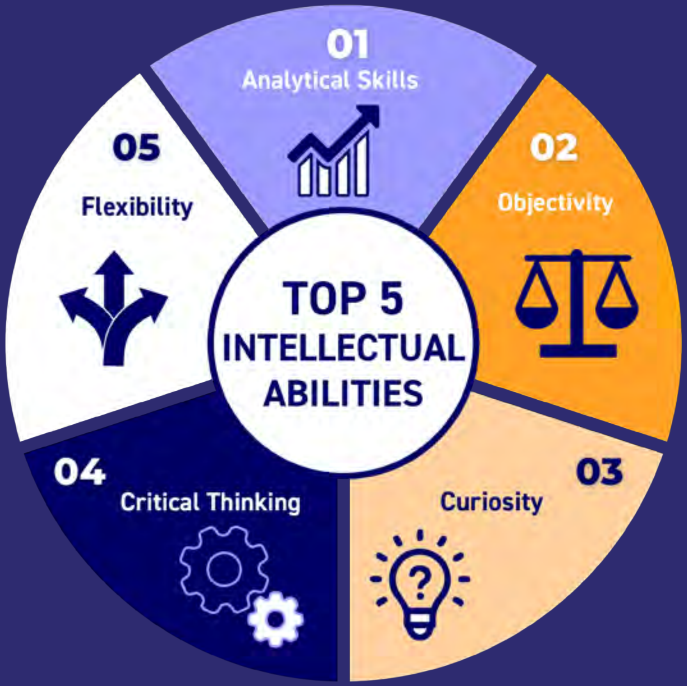
Some assessors also highlighted that specific knowledge of the terrorism field was desirable, as well as practical skills and experience such as supervision, interview techniques, and working with people.

It is likely that this range of training and experience reflects the diverse needs across the different disciplines and contexts involved in terrorism risk assessment (e.g. in the pre- or post-crime space). These findings also highlight the value of a multidisciplinary approach with mixed panels, which can bring a range of experience and knowledge to the process. Overarching training in specific tools and general risk assessment principles can help to bring these disciplines together.

ABILITIES AND CHARACTERISTICS

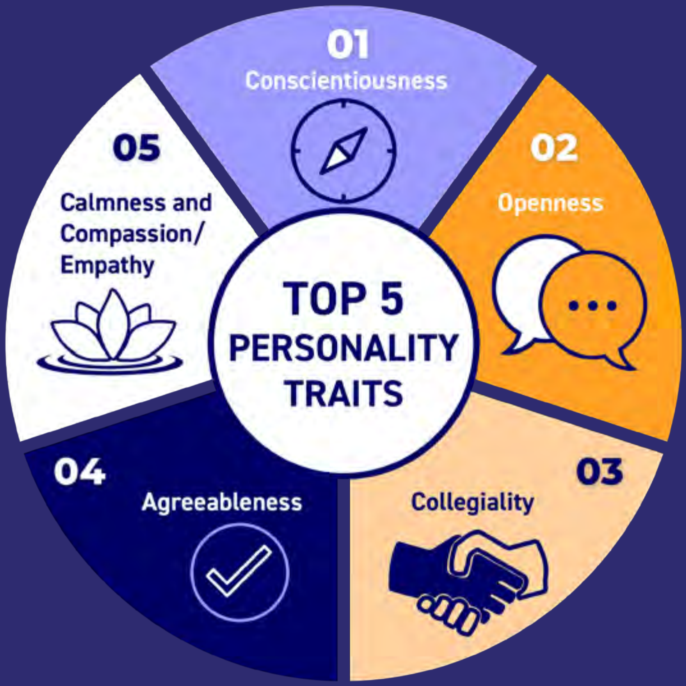
Finally, we asked assessors which intellectual abilities and personality characteristics they would expect of a 'good' risk assessor.

It could be said that possessing and developing these abilities and characteristics may be helpful to the risk assessment process. For example, findings from previous research suggest that more conscientious assessors may be more accurate and reliable in their judgments (Hanson et al., 2007). It is also possible that more personable assessors (i.e. collegial, agreeable, and compassionate) may build a better rapport with colleagues and service users. However, research is needed to evaluate the impact of these characteristics in practice.



PUTTING IT INTO PRACTICE

Our study findings indicate that there is no one-size-fits-all approach to terrorism risk assessment; the process and requirements for assessors will likely be guided by the context in which it takes place and the agencies involved. However, based on the opinions of practitioners, some general suggestions and considerations can be made for future practice and evaluation:



1. Risk assessment tools and SPJ protocols, and their training, should be designed with practitioners in mind, particularly considering their ease of use and availability.
2. Consideration should be given to the advantages, disadvantages, and practicability of in person or remote assessment. Consideration should also be given to the number of practitioners assessing each case – at least two may be optimal.
3. Professional training is more important than formal education. This could include training in the use of specific tools or protocols, as well as general principles of threat and risk assessment. Other training will depend on the context and discipline of the assessor, where multidisciplinary teams can bring a range of experience and skills to the assessment process.
4. Some intellectual abilities and personality characteristics may be helpful to the risk assessment process. More objective and conscientious assessors may be more accurate and reliable, while more personable approaches may improve rapport-building with colleagues and service users.

Nadine Salman is a Senior Research Associate in Psychology at Lancaster University and is completing her PhD in Security and Crime Science at University College London. Her research focuses on violent extremism risk assessment and management, risk and protective factors, and practitioner decision-making.

Professor Paul Gill is a Professor of Security and Crime Science at University College London. His research examines the behavioural underpinnings of terrorism and terrorist attacks.

CAROLINE LOGAN

VIOLENT EXTREMISM:

THE ASSESSMENT AND MANAGEMENT OF RISK

To date, the violent extremism literature has largely focused on the search to identify the (risk) factors thought to have the most bearing on an individual's decision to perpetrate an act of ideologically motivated violence. The field needs to evolve from this important but limited – and limiting – baseline.

This brief article presents eight recommendations for why and how practitioners and academics should develop from their current focus, using developments in the general risk and threat assessment field as an invaluable guide to the potential for improvement.

1. ACT ON YOUR ASSESSMENT

The sole purpose of risk assessment is to inform risk management – and the purpose of risk management is harm limitation at least or, at best, harm prevention. The assessment of risk without any intention of, or plan for, managing the concerns raised by the assessment should be regarded as both unethical and reckless.

> **It is not enough to compile lists of risk factors in the absence of attention to how evidence of their presence will be turned into a plan of preventative action based on the nature of the risks detected or suspected.**

2. TAKE A DYNAMIC APPROACH

The assessment and management of violent extremism risk is, or should be, a dynamic and real-time undertaking. Efforts to mitigate risk must inform the understanding evaluators have of its occurrence, which should, in turn, inform bespoke risk management in a continuous and circular process

> **Risk assessment and management is an ongoing, live, and dynamic process rather than one that is static or a snapshot in time.**

3. SEE THE BIGGER PICTURE

Risk factors for violent extremism, covering the range of internal (e.g. extremist ideology) and external (e.g. world events) experiences and responses, do not operate in isolation from other risk factors (e.g. a sense of grievance or threat, social support for an extremist world view, personal factors, etc.). Further, they do not operate in isolation from protective factors (e.g. barriers to action, non-extremist social support, etc.) or from the context in which they occur and are experienced.

> **The risk of an act of violent extremism is about the interplay – in an individual in a particular context and in real-time – of multiple risk and protective factors. This range of factors and their interplay should feature in risk assessment and management guidance in the violent extremism field as it does in other fields of harm prevention.**

4. SEEK A RANGE OF GUIDANCE

As with any risk, the risk of an act of violent extremism may be assessed at different points:

- at discovery
- at initial investigation
- at preparation and implementation of a risk mitigation plan
- at periodic reviews thereafter

This will continue until the risk is assessed to have achieved managed status and the case is closed to the lead agency responsible for its management. At that point, the case may be closed entirely, or it may be handed over to a partner agency to maintain or monitor that managed risk status over a prolonged period. For example, police may detect and initially manage the risk, and following management action, may hand over the case to mental health services to monitor if mental health problems were a particularly salient risk factor in the individual case.

Further, different agencies may have access to quite different kinds of information. For example, mental health practitioners may have direct access to the individual who is the subject of

concern, while law enforcement agencies may have less or indirect access only, but instead have access to a potentially rich vein of intelligence information that mental health practitioners may never see. Thus, each evaluation is a complex undertaking, requiring the balancing of multiple forms of evidence, dependencies, and contingencies that are relevant in different ways to the agencies involved.

Accordingly, a range of guidance in the assessment and management of violent extremism risk needs to be developed that will be sensitive to the requirements of different stages in the process in addition to evidence types as well as being aligned to one another to ensure continuity of case management across time and agency. Therefore, just as Ordnance Survey maps are available to travellers in different levels of granularity and focus for each of their regions, so too should there be a range of risk assessment and management guidance available to practitioners, from which they can choose according to need.

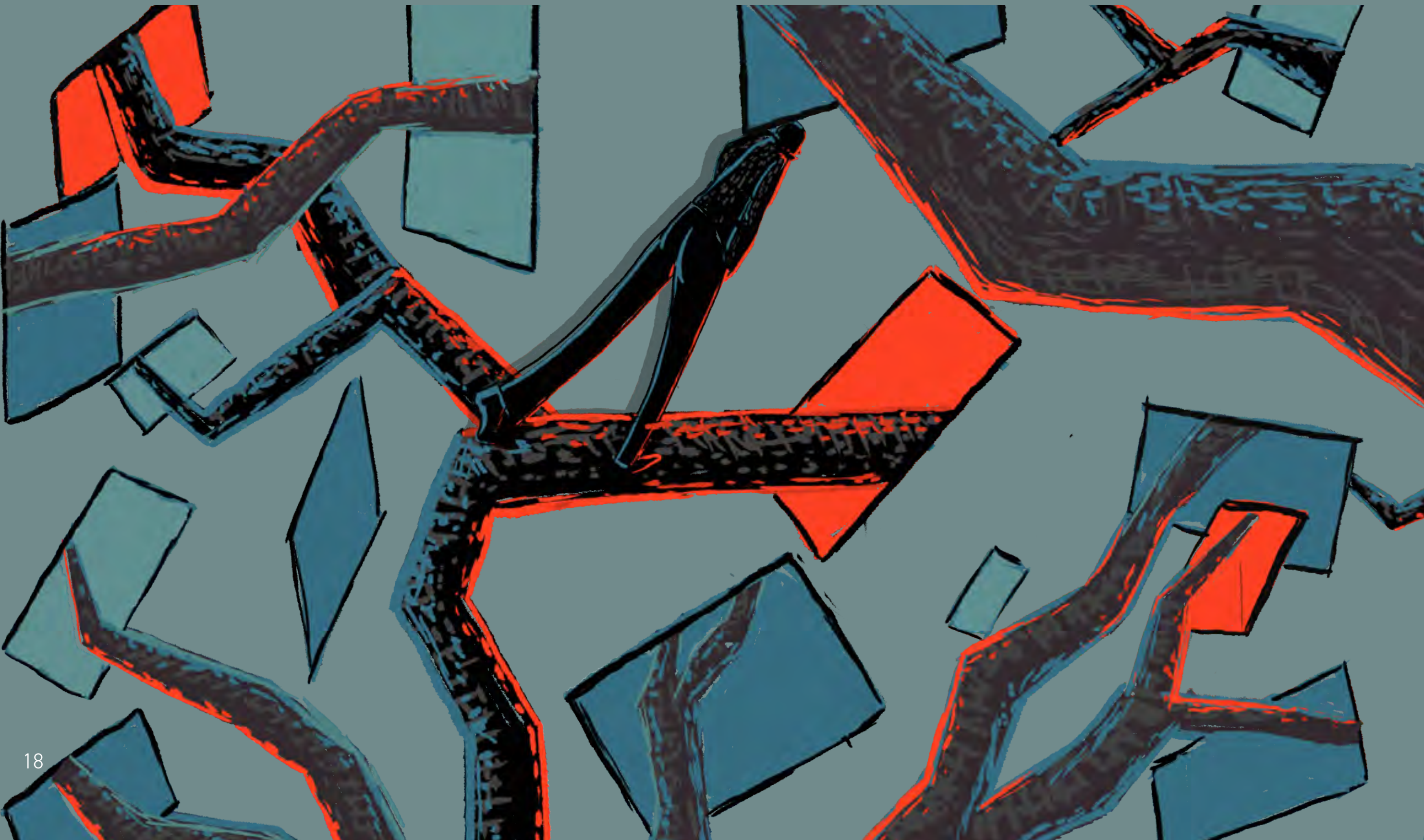
Practitioners in the violent extremism field should have available to them guidance that informs direct versus indirect assessments, guidance on in-depth assessments that will vary from that supporting long-term case management, guidance that supports the process of understanding the risks posed by individuals versus groups, and so on. The availability of a range of guidance – like maps of the terrain – is both good practice and a protection against the failure to take important variables and processes into consideration in the vital business of harm prevention (see Gawande, 2011 in Read More).

Different guidance (sometimes referred to as risk assessment tools or instruments) – focusing on different priorities and outcomes, from triage through to decisive action and review – is required at different stages in the task of understanding and managing individual risk. No single set of risk assessment and management guidance can achieve all the requirements of the process of preventing violent extremism.

5. TAKE THE SPJ APPROACH

Structured professional judgement (SPJ) is the recommended approach to the assessment and management of violent extremism risk (see Borum, 2015 and Monahan, 2015 in Read More). SPJ is an *approach* and not a specific set of risk assessment and management guidance or a particular tool or instrument. The SPJ approach requires investigators to identify the most relevant risk and protective factors in the individual case, using a synthesis of the empirical and professional research as their guide.

Based on what they have found out during the assessment stage, investigators are then required to articulate their hypotheses about individual risk potential and its motivational drivers (e.g. revenge, retribution, honour, esteem). Thus, the investigator tries to articulate *what* they think the person is at risk of and *why*, based on which a risk management plan is then designed and implemented. Its impact is used to inform further the investigator's understanding of the case and ongoing risk



The SPJ approach focuses on the whole person and not just on one or a limited selection of risk factors.

management. Consequently, the SPJ approach focuses on the whole person and not just on one or a limited selection of risk factors.

Several SPJ guidelines are available for practitioners, which embody the approach in different ways and to varying degrees of granularity; these are some of the first maps of this terrain.

The *Multi-Level Guidelines* fully operationalises the SPJ approach and to a very granular level. This guidance is suitable for use by practitioners experienced in understanding and communicating complex human behaviour (e.g. psychologists).

The *Extremism Risk Guidance-22+* (ERG-22+), the *Violent Extremism Risk Assessment-2 Revised* (VERA-2R;), and the *Terrorist Radicalisation Assessment Protocol-18* (TRAP-18;) operationalise SPJ partially – the guidance offered to practitioners to try to think through their understanding of the case and risk management planning is limited or, in the case of the VERA-2R and the TRAP-18, absent. (See Read More).

However, both the VERA-2R and the TRAP-18 have been written with law enforcement practitioners in mind, and these sets of guidance are more attuned to the interests of those professionals than any other. In contrast, the ERG-22+ is intended for the use of psychologists, although, at present, its use is limited to those who work in HM Prison and Probation Service in England and Wales.

> **Risk management should be about the person rather than their behaviour, and the SPJ approach intends to take practitioners towards the integrated individual and away from counting disarticulated behaviours. Guidance informed by the SPJ approach – such as the MLG, ERG-22+, VERA-2R and the TRAP-18 – helps ensure that practitioners do just this in the different settings in which they work.**

6. STUDY THE PROBLEM

Good practice in risk assessment and management requires an understanding of both the problem to be prevented (e.g. violent extremism) and the practice of risk assessment and management. Attendance at a training course in the application of a particular set of violent extremism risk assessment and management guidance will not make up for a poor understanding of violent extremism.

> **Expertise in one area is not a guarantee of good practice in the other. Practitioners who are competent risk managers must have proficiency in both risk assessment and the nature of the harm they are trying to prevent.**

7. BE TRANSPARENT

Risk assessment and management concerning violent extremism is an undertaking likely to be subject to the highest level of scrutiny by multiple agencies with competing agendas (e.g. police, security services, politicians, the courts, the media).

> **The task of assessing and managing risk should be transparent and accountable to facilitate reasonable scrutiny and defensible practice, nurturing continued support from these essential stakeholders.**

8. EVALUATE, EVALUATE, EVALUATE

Evaluation is critical to demonstrating good practice to key stakeholders, including the public who fund their protection through taxation and politicians who legislate for national security.

> **No process for understanding risk with a view to managing it should be implemented without regard for how improved practice may be measured and demonstrated.**

CONCLUSION

Risk assessment and management in the field of violent extremism is a complex undertaking. This brief article has considered some of those complexities and offered eight recommendations for their negotiation. Central to each recommendation is working in partnership, which is a vital requirement in the management of threats to national security. The SPJ approach lends itself to such cooperative working arrangements.

However, more diversity is required in the range of guidance available to practitioners to assess, understand, and manage the risk of violent extremism in all its forms, over time and working across agencies. In addition, more attention needs to be paid to the evaluation of risk management practices for us to know better what works in this field, and to move attention away from the identification of risk factors and on to the more substantial process of harm prevention (see Logan, Gill & Borum, in preparation in Read More).

Dr Caroline Logan is an Honorary Senior Lecturer at the University of Manchester.

BETTINA ROTTWEILER & PAUL GILL

RISK FACTORS FOR VIOLENT EXTREMIST BELIEFS AND PARALLEL PROBLEM AREAS

Does a strong conspiracy mentality lead to violent extremist intentions? Bettina Rottweiler and Paul Gill suggest it depends on the individual's self-control, law-related morality, and self-efficacy.

The growing evidence base for risk factors for violent extremism demonstrates many overlaps with parallel problem areas like domestic violence, mass murder, stalking, and threats to public figures. Increasingly, we are also witnessing a seeming convergence between belief in conspiracy theories and ideological extremes. This is most clearly evidenced by recent right-wing terrorist attacks in Hanau, Halle, Christchurch, El Paso, Pittsburgh and Poway. Each perpetrator's manifesto referenced conspiracies such as the great replacement theory or white genocide.

Belief in extreme ideologies and conspiracy theories are thought to be rooted in similar underlying psychology. Conspiracy theories and extremist ideologies are both fundamentally rooted in sense-making processes that aim to structure the world in a clear-cut manner and intend to reduce feelings of uncertainty amongst adherents. Both offer prescriptive and action-relevant guidance, with clearly defined values and morals.

Research in these two areas however largely remains siloed. Consequently, there is a dearth of empirical research on the relationship between conspiracy beliefs and violent extremism. In a German nationally representative phone survey (N = 1502), we sought to investigate the relationship in detail .

We asked each participant about the degree to which they agreed with:

1. Five generic themes that re-occur in different conspiracy theories (e.g. secret organisations greatly influence political decisions).
2. The scenarios under which they would be willing to engage in illegal and violent actions on behalf of a group they identify with.

In the German sample, almost 32% of respondents showed conspiracy beliefs and 8% held self-reported violent extremist intentions.

> "When stronger conspiracy beliefs are held in combination with high self-control and a strong law-relevant morality, violent extremist intentions are lower."

[As an aside, we asked the same questions in the U.K. in summer 2020, and 37% reported a conspiracy mentality and 12% demonstrated violent extremist intentions].

A structural equation model of German survey data confirm that a stronger conspiracy mentality leads to increased violent extremist intentions. However, moderator analyses demonstrated this relationship is contingent on several individual differences. The effects are much stronger for individuals exhibiting lower self-control, holding weaker law-related morality, and scoring higher in self-efficacy. Conversely, when stronger conspiracy beliefs are held in combination with high self-control and a strong law-relevant morality, violent extremist intentions are lower.

WHY IS THIS INTERESTING?

High self-efficacy isn't always positive

Self-efficacy is typically associated with positive outcomes, and prosocial intentions and behaviours. Here, we find the opposite. Individuals scoring highly in both conspiracy beliefs and self-efficacy may feel more capable of taking violent action to redress grievances. This is important for CVE interventions

Image credit | JessicaGirvan / Shutterstock.com

that solely focus on self-efficacy in order to make individuals more resilient to violent extremism. Such interventions need to simultaneously tackle underlying grievances as otherwise individuals might use their newly gained self-efficacy beliefs to act upon those strains.

High self-control and high law-related morality mitigates risk

For individuals with a high conspiracy mentality, both low self-control and low law-related morality present a risk factor for violent extremism. But the inverse is also true. High self-control and high law-related morality mitigate the movement toward violent extremist intentions, even when high conspiracy beliefs are present. This has major implications for how we think about protective factors. Both high self-control and high law-related morality can be defined as 'interactive' or 'buffering' protective factors that provide insurance when a risk factor (in this case conspiratorial beliefs) is present.

There is no silver bullet

Multiple factors contribute to a single individual's pathway into violent extremism. No single risk factor can explain its genesis. There is no silver bullet. Risk assessments, and the management strategies derived from them, must take account of the constellation of multiple factors that interact with (and sometimes enable or disable one another) rather than solely focusing upon single risk factors. This is a more subtle and nuanced art than numbers-driven actuarial approaches can currently achieve.

Multiple policies needed to encourage prevention

Preventing individuals with high conspiracy beliefs from becoming violently radicalised may necessitate tailored, rather than broadly generalised policies. If multiple trajectories into violent extremism exist, there should be multiple policies to encourage prevention. Not all policies will have relevance to all individuals presenting with similar conspiracy mentalities, as their constellation of other risk and protective factors likely differs.

Bettina Rottweiler is a Research Assistant and final-year PhD student in the Department of Security and Crime Science at University College London. Her PhD analyses risk and protective factors for violent extremist intentions using general population surveys.

Professor Paul Gill is a Professor of Security and Crime Science at University College London. His research examines the behavioural underpinnings of terrorism and terrorist attacks.

EMILY COLLINS, PHILLIP MORGAN & DYLAN JONES

IF THIS THEN...WHAT?

SECURITY AND PRIVACY IN TRIGGER-ACTION SYSTEMS

Can people be primed to think about security and privacy when setting trigger-action rules for smart home devices?

With the average UK household having more than ten Internet of Things (IoT) devices, more people are looking to find ways to connect apps and devices to create more complex systems in their homes. Trigger-action rules, such as those supported by IFTTT (short for If This Then That), are one way that this can be done.

IFTTT allows users to program a script – or 'applet' – to automate tasks, using some type of event in one app or device to trigger an output in another. For those who do not want to program their own, IFTTT estimate there are over 54 million existing applets available to download and deploy.

> "Users are often not able to anticipate or fully understand the security implications of these rules, especially when multiple rules create unpredictable knock-on effects."

The ease with which multiple applets can be created and simultaneously deployed presents several security and privacy issues. Users are often not able to anticipate or fully understand the security implications of these rules, especially when multiple rules create unpredictable knock-on effects – as they are often concentrating on their goal of automating a process or creating a convenient shortcut, safety can easily be pushed into the background.

Finding ways to encourage users to consider security and privacy when choosing these rules is important in maintaining safety.

Our research at Cardiff University looked at how people make decisions when selecting IFTTT rules and whether priming them in different ways might promote greater consideration of the security and privacy implications of the rules they choose.

First, we created a series of IFTTT rules and asked independent experts to rate each on security and privacy. For example, 'When the camera on my smart doorbell detects an unknown/suspicious person (e.g. someone who lingers on my property for over 20 seconds), send a photograph of that person and a text message to my neighbours'. This created a security and privacy score for each rule.

Our research asked participants to judge which of these rules they would enable in a given context through a game-based, experimental design. Some participants were just shown the rules, whereas others were primed to think about the security and privacy of the rules that they chose.

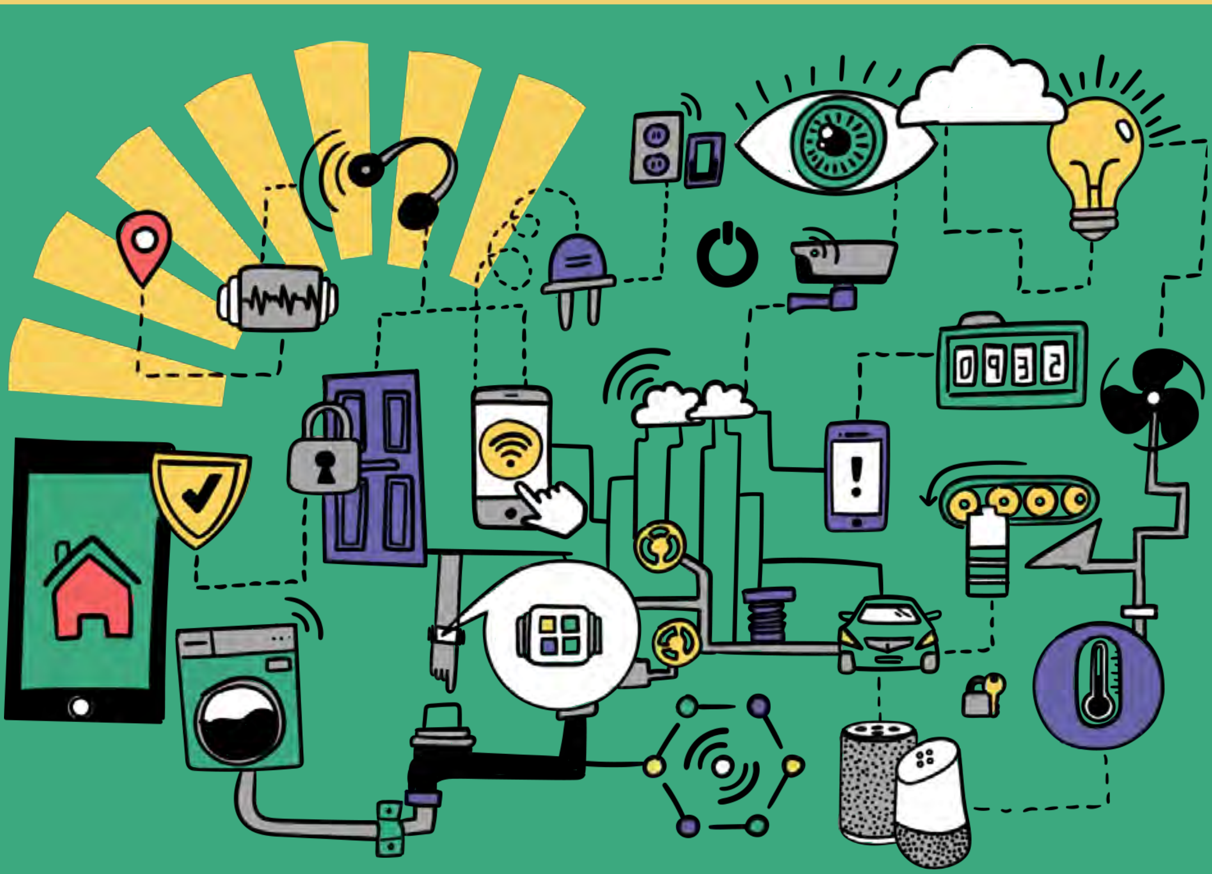
EXPLICIT PRIMING

In our first study, we used 'explicit priming', involving direct instructions to focus on either security or privacy. We found that these primes led to people choosing rules that were rated higher in security or privacy by our experts; security primes improved security scores and privacy primes improved privacy scores, although interestingly the security primes also led to lower privacy scores.

IMPLICIT PRIMING

In our second study, we used 'implicit priming' in the form of seemingly unrelated activities that involved solving a security or privacy problem. We found that these improved security scores, albeit less effectively than the explicit primes did. Overall, privacy and security priming were found to work in different ways depending on whether the priming was explicit or implicit.

Building on the work of our colleagues at the University of Bristol (What Influences Consumer Adoption and Secure Use of Smart Home Technology?), we also investigated whether



individual characteristics – namely propensity to adopt technology, perception of security risks, trusting beliefs, and privacy concerns – impacted people's choices.

FINDINGS

We found that users who showed greater awareness of the privacy practices of smart home companies tended to produce high security scores. They were less likely to take risks when enabling rules to connect devices and services.

> A preoccupation with privacy may encourage security to be neglected.

Increased concern about exercising control over personal information was associated with lower security scores, suggesting a preoccupation with privacy may encourage security to be neglected.

There were also strong suggestions that the more people trust online companies, or the more users expect to benefit from smart home technologies, the less likely they are to keep their personal information private. Enthusiasts for IFTTT and technology are more willing to put their privacy at risk, as one might expect. This shows how opinions that people hold about technology carry over to the choices they make when setting up smart home technology.

Overall, the findings of this project reinforce the importance of stressing the risks to security and privacy of IFTTT in smart home contexts. Consumers would benefit from more support in understanding how their systems are configured, as well as the potential knock-on effects of further device upgrades and additions, to facilitate the secure adoption of smart home technology.

Dr Emily I M Collins is a Lecturer in Human Factors at Cardiff University.

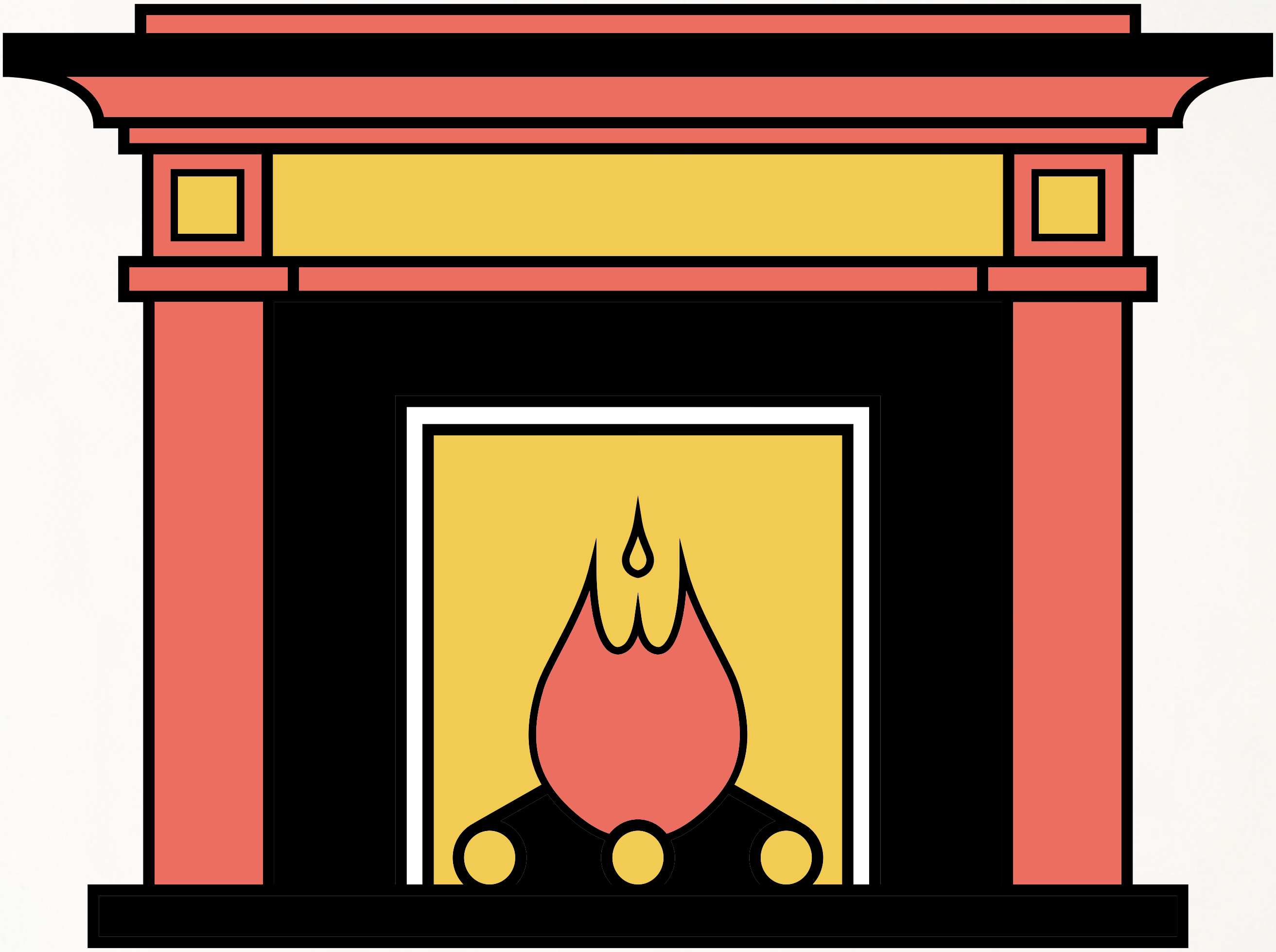
Professor Phillip L Morgan is a Professor in Human Factors and Cognitive Science within the School of Psychology at Cardiff University, Director of the Human Factors Excellence Research Group (HuFEx) and Director of Research within the AI, Robotics and Human Machines Systems Research Centre (IROHMS).

Professor Dylan M Jones is a Senior Professor within the School of Psychology at Cardiff University and Co-Director of HuFEx and IROHMS.

IAN STANIER & JORDAN NUNAN

IDENTIFYING INFORMANT MOTIVATION: THE FIREPLACES FRAMEWORK

A new framework has been developed to help law enforcement and intelligence agencies better identify and understand the motivations of informants.



Deployed informants are a vital tactic for law enforcement and intelligence agencies to identify and manage threats. Accurately identifying an informant's motivations for providing information enables informant handlers to better influence the informant's behaviour and reduce risks. In this article, Drs Ian Stanier and Jordan Nunan outline their mnemonic-driven framework.

WHY OFFER A MNEMONIC TO INFORMANT HANDLERS?

Mnemonics offer a strategy for learning by aiding the retention of important concepts. In doing so, they can help structure the analysis of complex information. Where the risky operating arena is fast-moving, such as when handling informants, mnemonics can reduce an officer's cognitive load of an already complex task.

This mnemonic aids the identification and diversity of informant motivation. It can be applied to improve an informant handler's awareness of the complexity of an informant's motivations, helping them to assess the types of motivations of potentially new informants and those in a continuing authorised relationship.

Building on existing mnemonics (e.g. MICE: Money, Ideology, Coercion, and Ego), the FIREPLACES framework highlights a broader scope of informants' motivations and acknowledges that motivation is not a fixed or singular concept. It explores the multidimensional nature of motivation and aims to promote the opportunities and identify the risks behind an informant providing information.

The FIREPLACES framework not only increases the probability of identifying motives but can also enhance control, efficacy, and longevity of authorised relationships; potentially increasing ethical intelligence elicitation.

THE EVIDENCE BASE

The range of motivations at play can be evidenced from a series of autobiographies and biographies of informants detailing their involvement in intelligence collection across both crime and terrorism fields.

> The FIREPLACES framework not only increases the probability of identifying motives but can also enhance control, efficacy, and longevity of authorised relationships; potentially increasing ethical intelligence elicitation.

Further affirmation on the diversity of motivations is drawn from research exploring the motivations recorded on informant source referrals submitted to Dedicated Source Units. This contemporary research challenged the narrower original MICE framework for the motivations of informants.

Additionally, research is underway exploring the United Kingdom's (UK) Domestic Extremism (DE) informants on their self-declared and informant handler assessed motivations for existing authorised DE informants. This has found that informants tend to hold a primary motivation for disclosing intelligence, although the majority also have secondary motivations for informing.

The data also supports earlier research that the motivation of informants is changeable during the period of the authorised relationship. The UK DE informant motivation research did not identify all forms of motivation within the framework (e.g. Coercion). However, the literature suggests that coercion has been a practice adopted by other countries so it was included to generate a framework that can be applied internationally.

THE FIREPLACES FRAMEWORK

Financial

Includes the receipt of monetary reward or in-kind payment (i.e. payment of rent, tools, vehicles, phones, clothes). One of the more common forms of motivation for authorised informants.

Ideology / Moral

Information is provided about a person or group who possess ideas or beliefs at odds with those held by the informant (i.e. a terrorist may start to question the validity of the original basis for their engagement with the terrorist group).

Revenge

Information is provided to harm or place another in a detrimental position (i.e. arrested) in response to a previous injury or perceived wrongdoing (i.e. as a result of an acrimonious breakup of a personal or criminal relationship).

Excitement

Undertaking the role of an informant offers the individual a feeling of excitement, eagerness, or arousal.

Protection

Passing information to authorities to protect the informant from persons or networks threatening them, their criminal enterprises, or their family. The cooperation aims to provide information that encourages police action to diminish this threat.

Lifestyle

The role played by the informant provides the individual with an enhanced lifestyle, either as a consequence of deployments and/or payments.

Access

The informant relationship provides an opportunity for counter-penetration to identify agency interest in offending networks and associates. This may include deliberate infiltration by criminals to understand the nature of police tasking and levels of interest in them or their competitor's criminal enterprises.

Coercion

Information is provided to avoid carrying out a threat made by an official (i.e. the threat of deportation; being prevented access to or from a country; or blackmail after being caught in compromising situations).

Ego

Undertaking the role of an informant enhances the individual's self-esteem or self-importance. Where this ego starts to impact the veracity of provided information, these are sometimes colloquially known as 'Walter-Mitty' informants.

Sentence

Information is shared to mitigate the length of a likely forthcoming prison sentence or release from detention. There is already UK legal precedent for rewarding people who provide intelligence to authorities.

UNDERSTANDING MOTIVATION AND ITS APPLICABILITY TO INFORMANT HANDLING

By gathering information about an informant's ambitions, fears, pursuits, morals, and perspectives, informant handlers can gain a greater insight into the informant's motivations. There are two key aspects of motivation:

1. Nature and direction of motivation – the reasons and decisions to act.
2. Magnitude of motivation – the commitment to pursuing an act.

> Informant handlers must not only discover the type of motivation(s) but also the strength of the motivator(s).

Informant handlers must not only discover the type of motivation(s) but also the strength of the motivator(s).

The FIREPLACES framework aims to assist the decision-making of law enforcement and intelligence agencies. The law concerning informant authorisation requires both regular reviews, and where appropriate, renewals of an informant's authority. The review process provides informant handlers with an opportunity to revisit the informant's motivations which may have evolved across singular or multiple motivations. This necessitates an examination of the informant's tasking activity, their general behaviour and demeanour, and the interrogation of open and closed datasets. All of these are explored to identify new and emerging risks alongside operational opportunities.

Understanding motivation also strengthens relationships. The cultivation of potential new informants and maintenance of existing relationships relies heavily on the application of rapport-building techniques. The identification of rapport-building 'hooks' (e.g. motivations, personal interests, and lifestyle characteristics) may influence cooperation. Within the context of HUMINT, rapport can be defined as 'developing and maintaining a working relationship with a human source by managing their motivations and welfare, while ensuring they understand the purpose of the relationship to secure reliable intelligence'. Furthermore, by identifying an informant's motivations, an informant handler can use this to their advantage by developing common ground to generate conversational topics that may elicit intelligence.

The benefits of identifying both the nature and extent of an informant's motivations include enhanced control over their activities and identifying and managing their vulnerabilities – ensuring safer future tasking deployments. Identifying an informant's motivations also helps ascertain the limits of their cooperation, the longevity of the relationship, and the potential for informant misconduct.

Accurate assessment of an informant's motivations for collecting and disclosing intelligence to their handlers supports the process for managing potential risks associated with subsequent deployments. For example, the identification of a potential motivation of revenge, while not in itself a barrier to recruitment, introduces elements of abundant caution into the informant-handler operational relationship.

It may generate additional cross-checking of the intelligence, more detailed questioning of the source, and further verification of answers centred on the provenance of the original information. This, in turn, assists with efforts to reduce, avoid, remove, or transfer identified risks.

Dr Ian Stanier is a Senior Lecturer at the Liverpool Centre for Advanced Policing Studies (LCAPS) at Liverpool John Moores University.

Dr Jordan Nunan is an LCAPS Associate Lecturer in the forensic elicitation of intelligence at Liverpool John Moores University.

BEN LEE

NARRATIVES OF THE FAR-RIGHT

Far-right narratives vary according to the beliefs of those telling them, but they often reflect common themes. In this article Ben Lee gives a short guide to narratives of the far-right.

Ideology is discussed openly in some parts of the far-right, but more commonly it is embedded in narratives. Narratives are often portrayed as factual, but the structure, cast of characters and focus of different narratives reveals something of the ideology that underpins them.

COMMON NARRATIVES

Narratives in the far-right vary according to the beliefs of those telling them, but they often reflect common themes:

ANTI-MINORITY NARRATIVES – That target minority groups threaten majority/native groups. This may include targeting specific ethnic minorities by linking them to criminality or questioning their intelligence. Far-right activism can also include amplifying mainstream news designed to cast target minority groups in a bad light.

DEMOGRAPHIC THREAT – That a combination of immigration and birth rates will result in the 'native' population becoming a minority in the near future. This narrative is closely linked to concepts such as 'white genocide' as well as the 'great replacement'. Anti-Muslim narratives also focus heavily on the demographic threat posed by Muslim immigration and birth rates as well as the perceived threat from Islamisation.

COLLAPSE – That some type of ethnic or cultural strife is inevitable as a result of the growing threat presented by minority groups. In neo-Nazi circles, this may manifest as 'race war'. Elsewhere this may be presented as predictions of civil war or civil disorder.

CONSPIRACISM –Conspiracy theories are defined as the belief that a small group of actors are working towards some malevolent end. Conspiracy theorising is common in large segments of the far-right. Anti-Semitic conspiracy theories in which a Jewish elite is envisaged as controlling world events (e.g. the idea of a Zionist Occupation Government (ZOG)) are common. In other areas, theories such as Eurabia, White Genocide, the Great Replacement, and the Kalergi plan are more prevalent.

ANTI-ELITE NARRATIVES – That the current political and social leadership bears responsibility for the current or coming crisis. For neo-Nazis, ruling elites are often presented either as Jewish or Jewish-controlled. In areas of the far-right, where anti-Semitic conspiracy theories are not endemic, this is often framed differently e.g. 'globalist', 'the left' or 'cultural Marxist'. The far-right also exhibits a collective sense of persecution, presenting themselves as victims of societal oppression.

HISTORICAL REVISIONISM – That key historical events have been distorted in the interests of suppressing far-right ideology. While this can be interpreted as a form of conspiracy theory, historical revisionism has been particularly prevalent in the form of Holocaust denial.

CONFLICTING NARRATIVES

Based on the above analysis, there are several clear points of conflict between different formations in the UK far-right:

BIOLOGICAL VS CULTURAL DISTINCTIONS – Some elements of the far-right are attempting to present themselves as shedding biological conceptualisations of race in favour of taking culture and identity as makers of belonging. This is a significant break with more traditional forms of racial nationalism.

NEO-NAZISM – The symbols, rhetoric and ideology of Nazism remain toxic. While there are some openly neo-Nazi formations in the UK, open support for Nazism is a taboo in other areas of the far-right.

ETHNO-PLURALISM VS SUPREMACY– Where race is taken as a central organising principle, different ideological positions draw competing conclusions. While neo-Nazis and related groups argue for white-supremacy, ethnopluralists argue instead for the need to preserve difference.

SUPPORT FOR DEMOCRACY – A key marker for distinguishing radical-right populists from the extreme right; the far-right, as a whole, varies on attitudes to democracy. This distinction needs to be treated with caution as understandings of democracy vary between groups and ideologies.

ESOTERICISM – Recent developments among extreme neo-Nazi groupings in the US and UK have revealed inherent tensions between secular or Christian-styled neo-Nazis and those who embrace more spiritual interpretations of neo-Nazism. The influence of the fascist Satanist group the Order of the Nine Angles, for example, has caused rifts in some groups.

Dr Ben Lee is a Senior Research Associate with CREST and is based at the Centre for the Study of Terrorism and Political Violence at the University of St Andrews.

"The far-right exhibits a collective sense of persecution, presenting themselves as victims of societal oppression."

NATHAN SMITH

RESILIENT PERFORMANCE OF DEFENCE AND SECURITY PERSONNEL

Our work provides new insights that can inform the measurement and training of personnel to help them perform resiliently in the volatile, uncertain, complex, and ambiguous (VUCA) environments they are tasked to operate in.

Personnel might encounter VUCA environments in remote and low resource areas of operation, like the conditions experienced in mountain or desert environments. They might also be exposed to VUCA conditions when working on the streets of a hostile area in a busy city, or even in a pressured cyber environment. Ultimately, the environments faced by defence and security personnel are demanding because the consequences of poor performance can have significant health and safety and broader strategic and political implications.

We have researched resilient performance in defence and security personnel with funding from the Human and Social Science Research Capability (HSSRC) and Defence Science and Technology Laboratory (DSTL). Our work has focused on bringing definitional clarity and exploring factors that affect whether an individual can perform resiliently under stressful conditions. We are using this information to design measurement tools and training programmes to enhance resilient performance.

RESILIENT PERFORMANCE MARKERS	APPLIED EXAMPLE
SKILLED MOTOR PERFORMANCES	MARKSMANSHIP
PHYSICAL FITNESS	ENDURANCE
PERSISTENCE AND EFFORT	BEHAVIOURAL INVESTMENT
JUDGEMENT AND DECISION MAKING	GO/NO-GO DECISION
ATTENTION AND CONCENTRATION	VIGILANT ATTENTION
COMMUNICATION SKILLS	INFORMATION ELICITATION

RESILIENT PERFORMANCE

Our work differs from the wider interest in resilience because it is principally focused on the issue of performance. Based on a systematic review of prior research findings, as well as semi-structured interviews with military, intelligence, and police firearms personnel (n = 17), we suggest resilient performance is 'the maintained or improved execution of competence under situational duress'.

With this definition in mind, we view resilient performance via changes in the competency markers relevant to the work of defence and security. This might include skilled motor performances, physical fitness, persistence and effort, judgement and decision-making, attention and concentration, and communication skills (see Table 1 for some applied examples). In our view, resilient performance is observed when personnel maintain or even enhance the required performance in these areas when placed under stress.

RESOURCE AND DEMAND PROCESSES

With resilient performance markers as outcomes, we can work backwards to examine factors that might affect performance. Proximal to specific performances are situational processes, reflected by in-the-moment psychological, social, and biological factors that determine whether someone is ready to perform or not. In our work, two overarching process dynamics were identified: resources and demands.

Resources include psychosocial elements such as perceptions of autonomy and control, competence and confidence, relatedness and trust, and self-regulation skills.

Demands are the specific situational features or risks that impinge upon in-the-moment performance and might include issues related to the physical environment, as well as sleep deprivation, information uncertainty, complexity, and social tensions.

Importantly for this work, it is the extent to which one perceives sufficient resources to meet or exceed the situational demands that determine whether performance is degraded, maintained, or improved. Greater perceived resources than demands underpin maintained and improved performance (resilient performance), while insufficient resources underpin performance decrements (non-resilient performance). This is in line with a transactional understanding of stress, whereby situations are rendered stressful by how individuals appraise

> Excessively high scores on certain variables, like mental toughness, might result in those factors becoming performance disablers.

the situation, and their capacity to cope within it (situation x appraisal = stress response inferred by biopsychosocial state).

ENABLERS AND DISABLERS

Zooming out from the situational level, various resilient performance enablers and disablers were identified in the literature and further explored in our end-user interviews. Based on current findings, we suggest that enablers and disablers are relatively stable global-contextual factors that influence performance by either bolstering or diminishing situational resources and demands.

Relatively high scores on trait-like factors such as the Big Five personality domains of conscientiousness, agreeableness, and openness, and high scores on adaptability, mental toughness, and hardiness are some of the performance enablers identified by the interviewees. Aspects such as intelligence and expertise were also pinpointed as contributing to performance.

There are some caveats, in that excessively high scores on certain variables, like mental toughness, might result in those factors becoming performance disablers. Other variables such as being ego-driven, arrogant, and overly neurotic were considered as disablers to performance.

While enablers and disablers are typically considered stable, practitioners we interviewed discussed how, in themselves and others, they have seen these factors change over time. This seemed especially so in the case of being exposed to formative and very challenging experiences, such as a demanding selection and training course or a stressful and potentially traumatic event.

NEW INSIGHTS

In contrast to polarising trait-like or process models of resilience, our findings suggest various global-contextual and situational variables are networked and will interact to dictate whether someone can perform resiliently or not. For example, enablers are predicted to impact resilient performance via their bolstering of situational resources. This is different to previous conceptualisations and moves beyond a view of resilience as either a disposition or something driven entirely by context.

With this suggestion in mind, we are cognizant of avoiding a 'fallacy of uniform efficacy', which is the assumption that more of something is always better. For instance, our interviewees highlighted that being too high on factors such as mental toughness or self-confidence might turn these commonly viewed performance enablers into disablers. In future work, we plan to examine these interactions to identify optimal levels and combinations of enabling variables.

Critically, we also acknowledge the importance of time. During our interviews, thinking about resilient performance over longer periods was repeatedly emphasised. This affirms the notion of consistency and the ability to execute relevant performance markers, or competencies, as and when called upon, over weeks, months, and years. This extended view is more robust to one-off performance breakdowns, which are likely inevitable, but that when viewed in isolation, might be used to label someone as 'not resilient'. A longer-term perspective also reinforces the dynamic temporal aspect of what it means to perform resiliently.

PROMOTING RESILIENT PERFORMANCE

Based on our suggestions, we are currently designing a battery of measures to assess global-contextual enablers (and disablers) and situational resource and demand processes that are proposed to underpin resilient performance. These measures will integrate psychological, social, and biological components. Initially, we will examine the predictive validity of the measured enablers, disablers, and processes on resilient performance markers assessed during ecologically valid stress tasks.

At the same time, we are developing a resilient performance training programme for defence and security personnel that draws upon prior work to offer novel blended learning on the topic. If and when validated, these parallel activities will provide the tools to both monitor and, through well-targeted interventions at both the global-contextual and situational level, enhance and sustain the resilient performance of defence and security personnel.

CONCLUSION

In a 2016 speech, Sir Alex Younger, former Chief of the Secret Intelligence Service, said that "We can put our officers where they need to be, in some of the most challenging locations imaginable, with the support they need to stay safe and the guidance and training required to navigate complex and ethically hazardous environments". Our work on resilient performance is designed to augment and extend the type of capability discussed by Younger. Ultimately, developing a scientific understanding that can inform evidence-based measurement tools and training to optimise resilient performance contributes to managing risk and empowers defence and security personnel to function effectively in the demanding VUCA environments they are tasked to operate in.

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

This work was produced with input from the wider project team, including Professor Marc Jones, Dr Elizabeth Braithwaite, Dr Martin Turner (Manchester Metropolitan University), Andy McCann (DNA Definite), Danielle Lefley-Burns (Manchester Metropolitan University), Dr Martin Jones and Dr Leonie Webster (DSTL).

SIMON OLESZKIEWICZ

THE ADAPTABLE LAW ENFORCEMENT OFFICER

What is adaptive behaviour? How can it be measured? And how do we determine its effectiveness?

In 2016 I was invited to observe two days of undercover training at the Los Angeles Police Department (LAPD). Before each training session, the undercover agents were provided with specific tasks to accomplish and then placed in various situations that demanded them to deal with awkward people while attempting to accomplish their objectives.

To say the least, I was impressed with the creativity and design of the complex social interactions that the undercover agents were trained to deal with. And, although a variety of behaviours were assessed for each scenario, in my view, one overarching behaviour stuck out across all scenarios: their ability to adapt.

THE IMPORTANCE OF ADAPTABILITY

When faced with novel or uncertain situations, the ability to adjust behaviour appropriately – the ability to adapt – is an invaluable skill. Adaptability is a central part of naturalistic decision-making and has been praised as a necessary condition of expertise.

However, despite extensive conceptual work on adaptability, no behavioural measure exists to evaluate the efficacy of adaptive responses.

So, what is adaptive behaviour? How can it be measured? And how do we determine its effectiveness? These questions consumed me for the next four years and inspired my colleagues and me to develop a novel experimental set-up for assessing and measuring adaptive behaviour.

THE SET-UP

In its most simple form, the set-up plays with three key features: an objective, an expectation, and a violation of that expectation.

Specifically, participants take on the role of an undercover agent who has to complete three mission objectives during a covert operation (e.g. collect the fingerprints of a study advisor). Importantly, the objectives cannot be changed or disengaged.

> “Participants take on the role of an undercover agent who has to complete three mission objectives during a covert operation.”

To give the agents an expectation, they receive a brief casefile before each mission providing some background information on the upcoming situation (e.g. a meeting has been arranged with the advisor and the agent has been tasked with collecting the advisor's fingerprints by making the advisor hold a paper with the agent's grades).

However, during each mission, the agent faces a social encounter that is inherently different from what has been described (e.g. new health rules require the advisor to wear gloves when holding received items). Hence, this expectancy violation creates a novel or unexpected situation that requires agents to adjust their behaviour (i.e. adapt to the situation) if they are to attain the mission objective.

MEASURING ADAPTABILITY

Having developed the experimental set-up designed to elicit adaptive behaviour, we needed a behavioural measurement of adaptability. However, to the best of our knowledge, one didn't exist. To overcome this, we drew on the theoretical definition of adaptability to explore several behavioural indicators that might be relevant.

Specifically, we examined how quickly agents make their first adjustment (adjustment onset) and how many times they adjust their behaviour (number of adjustments), on the assumption that both these measurements tap into the ability to generate alternative behaviours to adapt to a situation.

We also measured the average time spent on a specific strategy or behaviour (adjustment perseverance), on the assumption that spending too much time on an ineffective strategy is maladaptive. It may, for example, be reflective of decision inertia or an inability to generate alternative avenues of action.

We now had an experimental paradigm to elicit adaptive responses and a behavioural measure of the adaptive response. However, what we didn't know was whether adaptive responses aided in goal achievement.

THE FINAL PIECE OF THE PUZZLE

To complete the puzzle, we recruited a sample of 'granters' who were free to decide whether to grant or deny the agents' requests. Specifically, the granters were told they were to take part in a study examining new employees at the university (e.g. to consult other students on what courses to take next semester).

Importantly, what the granters didn't know was that their tasks were matched with the agents' missions (i.e. the granters were requested to wear gloves when receiving objects and items to reduce the spread of viruses). This allowed us to influence granters to unknowingly stand between the agent and the agent's mission objective.

With this experimental set-up, we ran our first study, in which mock undercover agents faced novel and unexpected situational demands while attempting to accomplish their mission objectives.

The agents' behavioural adaptability was measured as adjustments made in response to their changing situational demands, and the adaptability scale was used to complement this with a self-rated measure of adaptability.

However, one question remained: How might we estimate the practical value of the possible findings? To address this, we invited police officers experienced with covert policing to observe videos of the mock agents and assess their performance.

WHAT DID WE LEARN?

The experimental set-up successfully elicited adaptive behaviour as the agents were goal-oriented, perceived the missions to demand adaptive responses (rather than resilient or coping responses), and reported a need to adjust their behaviour to achieve their objectives. Moreover, adaptability was measured from three different perspectives – agents, granters, and observers – and each perspective provided unique insights.

From the agents' perspective, the findings suggest that self-rated adaptability might be important when facing novel and uncertain events, but that rating oneself as adaptable was associated with a less positive relationship with those the agent interacts with.

More specifically, from the granters' perspective, agents who rated themselves as adaptive tended to be perceived as lacking in benevolence (a feature of trustworthiness), suggesting that they may have come across as self-serving. Moreover, agents who succeeded in attaining mission objectives were rated as more able (another feature of trustworthiness) and more competent at developing rapport.

> **Adaptability (rated on the adaptability scale) is strongly connected with agents' trustworthiness and rapport.**

From the observers' perspective, adaptability (rated on the adaptability scale) is strongly connected with agents' trustworthiness and rapport and all three features are considered when predicting agents' success in accomplishing mission objectives. We interpret this finding as indicating that practitioners with covert experience deem that adaptability might not be functional without having established a positive relationship.

We also found initial evidence that behavioural adjustments might be a promising avenue for measuring behavioural adaptability. One of these measures – spending less time on each adjustment – showed a positive relationship with accomplishing mission objectives. This suggests that it might be valuable to consider the time that agents spend on each adjustment when assessing goal-oriented behaviour in novel and unexpected situations.

CONCLUSIONS

Although this study was a first explorative attempt to study behavioural adaptability, we tentatively suggest three preliminary conclusions:

1. Providing agents with a specific instrumental objective (e.g. collect the fingerprints of a study advisor) may lead to adaptive behaviour associated with a reduced relationship with those they interact with.
2. Practitioners seem to consider adaptability as being more a feature connected with the quality of the relationship than a feature for accomplishing mission objectives.
3. Practitioners should – but do not – take the time spent on each adjustment into account when assessing adaptability in novel and uncertain situations.

We believe that our development of the experimental paradigm to examine adaptability in a law enforcement context is a useful contribution of this research. By altering mission specifics within the schematic set-up of an objective, an expectation, and its violation, researchers should be able to examine an array of situations relevant to law enforcement contexts.

Dr Simon Oleszkiewicz is a Researcher at the Department of Criminal Law and Criminology at the Vrije Universiteit Amsterdam, the Netherlands.

MONICA LLOYD

THE A–Z OF EXTREMISM RISK ASSESSMENT

ACTUARIAL

A statistical calculation of the likelihood that an individual will pose a threat of future violence within a given period. It places an individual in a low, medium, or high-risk category based on characteristics that are known to contribute to risk of harm. There are currently insufficient known terrorist characteristics for extremist offenders and too few numbers to support such an approach to risk assessment for extremist violence.

BEHAVIOURAL VS COGNITIVE RADICALISATION

The distinction between adopting extremist beliefs (cognitive radicalisation) and acting on them (behavioural radicalisation).

CAPABILITY

The knowledge and skillset to execute a terrorist offence or make an effective contribution to a terrorist attack.

DYNAMIC VS STATIC FACTORS

The distinction between those factors that are subject to change, such as attitudes or beliefs (dynamic factors) and those that are fixed, such as criminal history or childhood experiences (static factors).

ENGAGEMENT VS DISENGAGEMENT

In risk assessment, 'engagement' covers emotional, ideological, and practical participation and involvement with extremist ideas and groups, in contrast to the loss or abandonment of an extremist ideology or the withdrawal or detachment from a group.

FORMULATION

A psychological assembling of the risk and protective factors underlying the problematic presentation of an individual that informs the targets and mechanisms for their change or management.

GROUP DYNAMICS

The impact on the thinking and behaviour of an individual within a group with whom they are closely identified, and that can contribute to both their cognitive and behavioural radicalisation.

HARM PREVENTION

The goal of risk or threat assessment that requires precise knowledge about the risk of harm to whom and in what circumstances, to inform risk management.

INTENT

The mindset that corresponds with the shift from cognitive to behavioural radicalisation and the decision to carry out or contribute to a terrorist offence.

JUDGEMENT

The process by which one arrives at a risk assessment decision that takes into account the individual's level of engagement, motivation, and intent to commit an extremist offence. It refers to the element of discernment required in every risk decision that relies on professional expertise and that renders risk assessment an inexact science.

KNOWLEDGE

The acquired knowledge of relevant risk factors for terrorism from a) academic research that shows an association between a specific factor and a terrorism risk, b) the experience gained from assessing and managing terrorism cases, and c) knowledge of the psychology of human behaviour and the needs met by extremist engagement and terrorist violence.

LONE ACTORS VS GROUP ACTORS

Lone actors are those who act alone in committing an extremist offence outside of any command and control structure and without the assistance of others. They may share a group ideology but are not embedded in a terrorist group, and are more often driven by a personal issue not shared by others.

MULTIFINALITY AND EQUIFINALITY

These are terms used in terrorist risk assessment that refer to the processes by which individuals can arrive at the same destination by many different routes (equifinality) and by which those with similar starting points can end up at different destinations (multifinality).

NARCISSISM

Narcissism was considered for some time to be a master explanation for terrorism. Extremist ideologies promise supremacy and there is some evidence that those with exaggerated self-importance are attracted to them for this reason. It is now viewed more proportionately as one of the personality features associated with terrorist group leaders and some lone actors who fail – perhaps because of their self-centeredness, to embed in a group.

OUTCOME STUDIES

Outcome studies in terrorism research seek to evaluate and optimise the outcomes of risk assessment and its management, as well as interventions with terrorist offenders, with the long-term goal of identifying what works.

PROTECTIVE FACTORS VS RISK FACTORS

Protective factors are the antidote to risk factors and are an essential element in the assessment and management of the threat of extremism. They decrease the chances of risk factors emerging and mitigate them where they do. The risk factors for terrorism apply to many others who hold similar grievances and have failed to find their place in society but who have not become extremists. It can be the factors that are key to understanding how they have been protected from this pathway.

QUALITY ASSURANCE AND QUALITY CONTROL

For frameworks that structure and guide extremist risk assessment, quality assurance is achieved through studies that measure their reliability (the consistency of their performance when used by different assessors) and their validity (from outcome studies that confirm that the frameworks are actually measuring what they purport to measure). Quality control is achieved by ensuring that those who use these frameworks are suitably trained and experienced in their use.

RELIABILITY

Reliability refers to the dependability of risk assessment frameworks. It is evaluated by studies that check the inter-rater reliability of those using the framework independently but in the same setting and with the same type of people. Reliability is expressed in Kappa values from 0.4 to 1.0, with values 0.6 and above corresponding with moderate to perfect agreement.

STRUCTURED PROFESSIONAL JUDGEMENT (SPJ)

SPJ is an approach to risk assessment that structures professional judgement by means of evidence-based guidelines. These provide a set of operationally defined and evidence-based risk factors, coding procedures for assessing their relevance to the individual case, and guidance for how to integrate these to reach a final decision about risk.

THREAT ASSESSMENT

Threat assessment takes place before an offence has been committed and is concerned to detect it and prevent it occurring. It is carried out by police and intelligence analysts. This is distinct from risk assessments that take place after an offence has been committed and are concerned to assess the potential of an already convicted offender reoffending in the future. It is carried out by correctional professionals in prisons or other secure settings.

UTILITY

Utility captures the value of a risk-assessment framework to its stakeholders. It corresponds to the extent to which they believe that the risk decisions it informs are superior to those that are made without it. It is a necessary but insufficient measure of the worth of a risk assessment tool.

VALIDITY

Validity is the gold standard for a risk assessment tool. It provides stakeholders with the confidence that it measures what it purports to measure and that its findings are meaningful. Ongoing outcome studies provide a continuing source of feedback to maintain confidence in its validity.

WHAT WORKS

This refers to the evidence base that accrues from systematically evaluating the outcome of correctional practice in the assessment and management of risk. The utility of a risk assessment framework cannot be assumed but needs to be evidenced.

X

A 'classic' formula used to describe generic risks from natural and man-made hazards is: Risk = Threat x Vulnerability x Consequence. Historically, such formulae were used to set priorities for protecting infrastructures against natural hazards such as flooding and hurricanes. However, the 'x' is controversial when considering terrorism risk. For terrorism risk to infrastructures, such formulae may be inadequate because threats, vulnerabilities, and consequences may not be independent with feedback loops existing between these factors due to the actions of intelligent adversaries.

YOUTH

Increasingly the caseload of Channel/Pursue referrals includes teenagers. Risk assessment and management strategies may need to be tailored for adolescent populations because their risk/protective factors and intervention needs may differ from adults.

ZERO RISK

All activity carries some risk. The only way to ensure zero risk is to allow no activity at all. Assessments gauge whether the level of risk is acceptable and manageable in the political and social context in which it may manifest.

Monica Lloyd is a Senior Lecturer in Forensic Psychology at the University of Birmingham.

READ MORE

Want to read more about some of the research that our contributors mentioned in their articles? Take a look below. We've flagged up those that are open access and given links to online versions where they are available.

CAROLINE LOGAN - VIOLENT EXTREMISM: THE ASSESSMENT AND MANAGEMENT OF RISK

Borum, R. (2015). Assessing risk for terrorism involvement. *Journal of Threat Assessment and Management, 2*, 63–87.
🔓 Available at: tinyurl.com/kzwr3r9h

Cook, A.N., Hart, S.D., & Kropp, P.R. (2013). *Multi-Level Guidelines (MLG) for the assessment and management of group-based violence*. User Manual. Burnaby, BC: Mental Health, Law, and Policy Institute. 🔓 Available at: tinyurl.com/3mffasy9

Gawande, A. (2011). *The checklist manifesto*. London: Profile Books Ltd.

Lloyd, M., & Dean, C. (2015). The development of structured guidelines for assessing risk in extremist offenders. *Journal of Threat Assessment and Management*, *2*, 40–52. doi: 10.1037/tam0000035

Logan, C., Gill, P., & Borum, R. (in preparation). *Violent Extremism: A handbook of risk assessment and management*. London: University of London Press

Meloy, J.R., & Gill, P. (2016). The lone-actor terrorist and the TRAP-18. *Journal of Threat Assessment and Management*, *3*, 37–52. doi: 10.1037/tam0000061

Monahan, J. (2016). The individual risk assessment of terrorism: Recent developments. *Virginia Public Law and Legal Theory Research Paper*, *57*. doi: 10.2139/ssrn.2665815
🔓 Available at: tinyurl.com/yp9scyyk

Pressman, E., et al. (2016). *VERA-2R Violent Extremism Risk Assessment Version 2 Revised: A Structured Professional Judgement Approach*. Utrecht, The Netherlands: NIFP/DJI

DAVID MCILHATTON & RACHEL MONAGHAN - PROTECTING PUBLICLY ACCESSIBLE LOCATIONS FROM TERRORISM

Home Office (2021). *Protect Duty Consultation: Making the public safer at publicly accessible locations*.
🔓 Available at: www.gov.uk/government/consultations/protect-duty

McIlhatton, D., et al. (2019). Protecting Commercial Real Estate and Crowded Places from Terrorism. *Journal of Real Estate Literature*, 27(1), 103–116. 🔓 Available at: tinyurl.com/2cw9hjpm

McIlhatton, D., et al. (2020). Protecting Crowded Places from Terrorism: An Analysis of the Current Considerations and Barriers Inhibiting the Adoption of Counterterrorism Protective Security Measures, *Studies in Conflict & Terrorism*, 43(9), 753–774.
🔓 Available at: tinyurl.com/2fva44p4

NADINE SALMAN & PAUL GILL - TERRORISM RISK ASSESSMENT: WHAT MAKES A 'GOOD' RISK ASSESSOR?

Hanson, R. K., et al. (2007). *Assessing the risk of sexual offenders on community supervision: The Dynamic Supervision Project*. Ottawa, Ontario: Public Safety Canada.
🔓 Available at: tinyurl.com/s8m5h4j5

Salman, N. L., & Gill, P. (2020). A survey of risk and threat assessors: Processes, skills, and characteristics in terrorism risk assessment. *Journal of Threat Assessment and Management*, 7(1-2), 122–129.

BROOKE ROGERS, ET AL. - INCREASING THE EFFECTIVENESS OF PUBLIC COMMUNICATIONS ABOUT TERRORIST ATTACKS IN CROWDED PLACES

Lindekilde, L., et al. (2021). 'Run, Hide, Tell' or 'Run, Hide, Fight'? *International Journal of Disaster Risk Reduction*, 60(15), 1-9.

Pearce, J.M., et al. (2019). Communicating with the public about marauding terrorist firearms attacks: Results from a survey experiment on factors influencing intention to 'Run Hide Tell'. *Risk Analysis*, 39(8), 1675-1694. doi: 10.1111/risa.13301

Pearce, J.M., et al. (2019). Encouraging public reporting of suspicious behaviour on rail networks. *Policing and Society,* 60(7), 835-853. Published online: 19 April 2019. 🔓 Available at: tinyurl.com/7nnw6bc6

STEVEN WATSON - RISK, BENEFITS, AND THE AFFECT HEURISTIC IN SECURITY BEHAVIOURS

Epstein, S. (1994). Integration of the cognitive and the psychodynamic unconscious. *American Psychologist, 49*(8), 709.

Lichtenstein, S., et al. (1978). Judged frequency of lethal events. *Journal of experimental psychology: Human Learning and Memory, 4*(6), 551.

Pham, M. T., & Avnet, T. (2009). Contingent reliance on the affect heuristic as a function of regulatory focus. *Organizational Behavior and Human Decision Processes, 108*(2), 267-278.

Slovic, P., et al. (2004). Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk Analysis, 24*(2), 311-322. 🔓 Available at: tinyurl.com/drnyfbyw

Slovic, P., et al. (2007). The affect heuristic. *European Journal of Operational Research, 177*(3), 1333-1352.
🔓 Available at: tinyurl.com/b999wz7t

Watson, S. J., Zizzo, D. J., & Fleming, P. (2014). *Determinants and Welfare Implications of Unlawful File Sharing: A Scoping Review* (Working Paper 2014/05). CREATe.
🔓 Available at: tinyurl.com/4wx2yvs8

Watson, S. J., Zizzo, D. J., & Fleming, P. (2017). Risk, benefit and moderators of the affect heuristic in a widespread unlawful activity: Evidence from a survey of unlawful file sharing behavior. *Risk Analysis*. 🔓 Available at: *tinyurl.com/wwbyj3zu*

IAN STANIER & JORDAN NUNAN - IDENTIFYING INFORMANT MOTIVATION: THE FIREPLACES FRAMEWORK

Nunan, J., et al (2020). The impact of rapport on intelligence yield: police source handler telephone interactions with covert human intelligence sources. *Psychiatry, Psychology and Law*, 1-19. 🔓 Available at: *tinyurl.com/5yeshjjc*

Stanier, I., & Nunan, J. (2018). Reframing intelligence interviews: The applicability of psychological research to HUMINT elicitation. In *The Psychology of Criminal Investigation,* 226-248. Routledge.

Stanier, I., & Nunan, J. (2021). The impact of COVID-19 on UK informant use and management. *Policing and Society,* 1-18. 🔓 Available at: *tinyurl.com/wyfn27up*

BETTINA ROTTWEILER & PAUL GILL - RISK FACTORS FOR VIOLENT EXTREMIST BELIEFS & PARALLEL PROBLEM AREAS

Douglas, K. M. (2021). Are conspiracy theories harmless? The Spanish Journal of Psychology, 24. 🔓 Available at: *tinyurl.com/ywadkkj8*

Hoyle, A., et al. (2021). Grey matters: Advancing a psychological effects-based approach to countering malign information influence. *New Perspectives*, 29(2), 144-164.

Rottweiler, B., & Gill, P. (2020). Conspiracy Beliefs and Violent Extremist Intentions: The Contingent Effects of Self-efficacy, Self-control and Law-related *Morality. Terrorism and Political Violence*, 1-20.

Rousis, G. J., Richard, F. D., & Wang, D. Y. D. (2020). The Truth Is Out There: The Prevalence of Conspiracy Theory Use by Radical Violent Extremist Organizations. *Terrorism and Political Violence,* 1-19. 🔓 Available at: *tinyurl.com/2nsnwpn6*

SIMON OLESZKIEWICZ - THE ADAPTABLE LAW ENFORCEMENT OFFICER

Klein, G., et al. (2014). The Good Stranger frame for police and military activities. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 58(1), 275–279. Los Angeles, CA: SAGE Publications

Martin, A. J., et al. (2012). Adaptability: Conceptual and empirical perspectives on responses to change, novelty and uncertainty. *Australian Journal of Guidance and Counselling*, 22, 58–81

Martin, A. J., et al. (2013). Adaptability: How students' responses to uncertainty and novelty predict their academic and non-academic outcomes. *Journal of Educational Psychology*, 105, 728–746

Martin, A. J. (2017). Adaptability – what it is and what it is not: Comment on Chandra and Leong (2016). *American Psychologist*, 72, 696–698

Ward, P., et al. (2018). Adaptive skill as the conditio sine qua non of expertise. *Journal of Applied Research in Memory and Cognition*, 7, 35–50

EMILY COLLINS, ET AL. - IF THIS THEN...WHAT? SECURITY AND PRIVACY IN TRIGGER-ACTION SYSTEMS

Mapping Smart Home Vulnerabilities to Cyber-Enabled Crime 🔓 Available at: *tinyurl.com/4p2fr98b*

What Influences Consumer Adoption and Secure Use of Smart Home Technology? 🔓 Available at: *tinyurl.com/y2as4mzf*

BEN LEE - A SHORT GUIDE TO NARRATIVES OF THE FAR-RIGHT

Archer, T. (2013). 'Breivik's Mindset: The Counterjihad and the New Transatlantic Anti-Muslim Right'. In Taylor, M. Currie, P., and Holbrook, D., (eds) *Extreme Right Wing Political Violence and Terrorism*, London: Bloomsbury Academic. 169–185

Barkun, M. (2003). *A culture of conspiracy: apocalyptic visions in contemporary America.* Oakland: University of California Press.

Hobbs, M (2018). 'The Men who Rewrite History': Holocaust Denial and the British far-Right from 1967. in Copsey, N and Worley, M (eds) *'Tomorrow Belongs to Us': the British Far-Right Since 1967*. London: Routledge. 9-26.

Hope Not Hate (2019). *State of Hate 2018: People vs the Elite?* 🔓 Available at: *tinyurl.com/2czf6k7p*

Jackson, P. (2013). The License to Hate: Peder Jensen's Fascist Rhetoric in Anders Breivik's Manifesto 2083: A European Declaration of Independence. *Democracy and Security*, 9(3), 247–269. 🔓 Available at: *tinyurl.com/42rzuwft*

Lee, B. (2015). A Day in the "Swamp": Understanding Discourse in the Online Counter-Jihad Nebula. *Democracy and Security*, 11(3), 248–274. 🔓 Available at: *tinyurl.com/ysxkztes*

Lipstadt, D. (1993). *Denying the Holocaust: The Growing Assault on Truth and Memory*. London: Penguin.

Meleagrou-Hitchens, A., & Brun, H. (2013). *A Neo-Nationalist Network: The English Defence League and Europe's Counter-Jihad Movement*. London: ICSR. 🔓 Available at: *tinyurl.com/3bpjvwxu*

Mudde, C. (2007). *Populist Radical Right Parties in Europe*. Cambridge: Cambridge University Press.

Pilkington, H. (2016). *Loud and proud: Passion and politics in the English Defence League*. Manchester: Manchester University Press.

Wendling, M (2018). *Alt-Right: From 4chan to the Whitehouse*. London: Pluto Press.

Zúquete, J. P (2018). *The Identitarians: The Movement Against Globalism and Islam in Europe*. Notre Dame: Notre Dame Press

NATHAN SMITH - RESILIENT PERFORMANCE OF DEFENCE AND SECURITY PERSONNEL

For further reading see *CREST Security Review,* issue 10, Stress and Resilience. 🔓 Available at: *tinyurl.com/n4ryu9w3*

CREST
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 and find us on Twitter, @crest_research

Lancaster University
UNIVERSITY OF PORTSMOUTH
UNIVERSITY OF BATH
UKRI Economic and Social Research Council