AUTUMN 2024 / ISSUE 19

CREST SECURITY REVIEW

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

Deterrence

CONTENTS

CREST SECURITY REVIEW
Editor – Rebecca Stevens
Co-Editor – Kayleigh Brennan
Illustrator & designers – Rebecca Stevens, Kayleigh Brennan, & Steve Longdale
To contact *CREST Security Review* email
csr@crestresearch.ac.uk

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

FROM THE EDITORS

Successfully deterring individuals from engaging in behaviour that poses security threats demands a deep understanding of what motivates harmful actions. By examining the social and psychological drivers behind these risks, we can develop more effective strategies to prevent them.

In this issue of *CREST Security Review*, we explore how cutting-edge research is transforming deterrence, from mitigating insider threats to combating cybercrime.

We begin with Shaw (p. 4) who provides an overview of recent developments of the Critical Pathway to Insider Risk™. Staying on the topic of insider risk, Martin (p. 8) attempts to distil the complex issues into a set of ten simple principles.

Next, Nurse (p. 12) proposes an effective ransomware deterrence strategy which could re-define cyber deterrence more widely.

On p. 14, Marchment explores the existing evidence base on crime displacement and benefit diffusion.

Squires' research (p. 16) begins to explain the differences in the types of crimes men and women are prosecuted for, the sentencing differences, and the implications.

Meanwhile, McIlhatton's research project (p. 18), responds to the challenge of understanding how best to evaluate protective security measures in an increasingly complex threat environment.

On p. 22, Grubin sparks a debate on whether polygraph testing in a police environment should be put to wider use.

Bystanders are often key to preventing acts of mass violence. However, as Cilke and Rowe (p. 26) discuss, education and awareness for security professionals and authorities in bystander reporting is needed to understand the barriers they face.

Additionally, Thomas and Grossman (p. 24) share their upcoming international policy-focussed research study on community reporting thresholds.

Finally, Benson (p. 28) explains that a multi-pronged strategy is needed to deter and prevent illicit finance.

Additionally, we feature articles addressing broader aspects of security research. Czerwinsky (p. 30) examines the entry pathways into misogynist 'inceldom' and subsequent considerations for practitioners. While Luther, Eastwood, and Snook (p. 32) discuss the effectiveness of using sketching as an interview tool.

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

Rebecca Stevens & Kayleigh Brennan
Editors, *CSR.*

GIVE US YOUR FEEDBACK!

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

www.crestresearch.ac.uk/csr-survey

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

ERIC D. SHAW

FROM RESEARCH TO PRACTICE AND BACK AGAIN:

IMPLICATIONS OF THE CRITICAL PATHWAY TO INSIDER RISK FOR CURRENT PERSONNEL SECURITY PRACTICES

Eric D. Shaw provides an overview of recent development of the Critical Pathway to Insider Risk™, highlighting the critical role that practitioners have had in its evolution.

INTRODUCTION

The Critical Pathway to Insider Risk™ (CPIR) describes the personal predispositions past insiders have brought to their organisations (personality and psychiatric issues, previous violations, social network risks), the triggers or stressors that have stimulated higher levels of insider risk, the concerning behaviours that signal observable behavioural indicators of increased insider risk in the workplace, the often maladaptive organisational responses that have failed to deter insider risks and the crime scripts that have accompanied insider actions.

It was described in detail by Shaws and Sellers and has been the focus of significant development and review by practitioners and researchers over the past 20 years. Since 2015, the CPIR™ has been frequently incorporated into discussions of insider actions and methods for detection of insider risk. Lenzenweger and Shaw (2022) summarised this development of the CPIR™, its strengths and weaknesses and reasons for its wide acceptance. This work summarises recent evolution of the framework and highlights direct implications for Personnel Security policies and practices.

FROM PRACTICE TO RESEARCH: THE EVOLUTION OF THE CPIR™

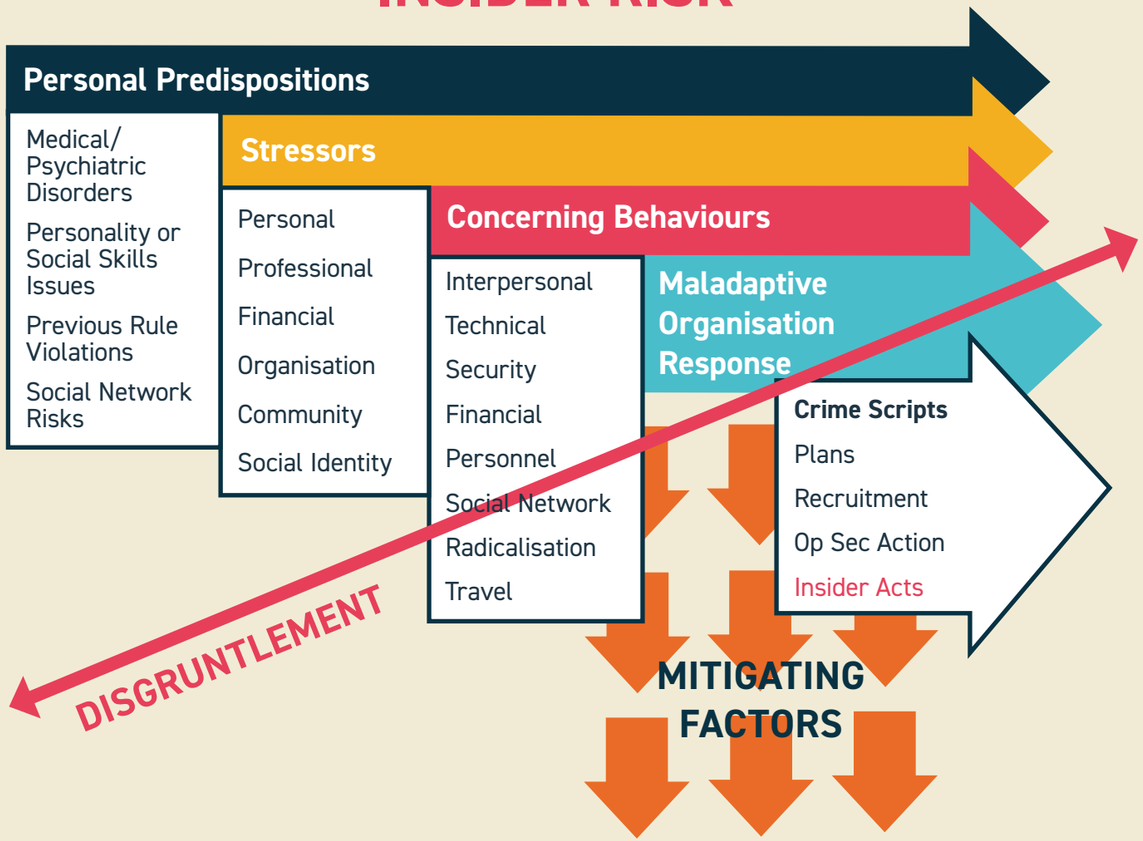
The CPIR™ framework is a living document. It has evolved as a direct result of feedback and engagement from insider risk professionals. Over 2,000 practitioners have participated in interactive CPIR™ training worldwide and have directly contributed to the framework's development based on their experience. Examples of these contributions, subsequent modifications, and questions include:

- The addition of Organisational Stressors to the Stressor Category as a trigger for heightened insider risk. Instead of concentrating on individual stressors alone, we have learned that leadership changes or controversy, mergers, redundancies, and other organisational changes often impact employee risk drivers;
- The addition of the Community Stressor category, which focuses on events impacting entire communities, also drives employee risk. No experience drove the important impact of these stressors home more than the COVID-19 Pandemic, which resulted in an increase in personal, family, financial, social, professional, and financial stressors to employees;
- Within the category of Community Stressors, the addition of Social Identity Stress (SIS). Based on the work of Veenstra, which focusses on normative conflicts between employees and their organisations increasing insider risk (such as employee disgruntlement regarding Pandemic public health interventions at work);
- The improved development of SIS and its implications for Social Network Risks, Concerning Behaviours, Problematic Organisational Responses, and the Mitigator of Enlightened Management. SIS can increase the likelihood of Social Network Risks as Concerning Behaviours, managers can over-react to non-threatening network risks causing risk escalation, and Enlightened Management must now understand and communicate with employees regarding potential SIS, in addition to their personal risk issues. Our team are currently working on ways to better identify and assess SIS;
- Despite the relative strength of controlled research demonstrating the relationship between personality disorder traits and insider risk, the addition of immaturity (divided into naivete, as in the case of Clayton Lonetree, and gullibility, as in the case of Sharon Scrange) into the Personal Predispositions category;
- While therapy often succeeds in reducing risk, we have also highlighted many cases in which therapy did not deter or prevent insider acts, and without information on its effectiveness, may not prove a risk mitigator. Security managers are urged not to assume that an employee in therapy is no longer a potential insider;
- Attention to the possibility that suicidal ideation, marking a period of intense hopelessness, despair and need for relief, may prove a gateway into increased insider risk among the estimated 90% of persons who experience suicidal ideation but do not go on to take their lives. We have begun to collect data on insiders who experienced suicidal ideation prior to their violations and noted the relative frequency of such ideation in targeted and domestic violence, as well as in espionage subjects. We are also increasingly focused on better ways to detect suicide risk in the complex communication patterns of the estimated 50% of persons who kill themselves without overt references to self-harm in their communications.

These are currently useful hypotheses regarding the causes, motives, and pathways of insider risk, but may be immediately relevant for practitioner consideration. We welcome feedback from reader's own observations.

> **Over 2,000 practitioners have participated in interactive CPIR™ training worldwide and have directly contributed to the framework's development based on their experience.**

Image credit: © *natashapankina* | stock.adobe.com



FROM RESEARCH TO PRACTICE: THE DEVELOPMENT OF INVESTIGATIVE TOOLS

The CPIR™ has contributed to the development of several tools designed to assist analysts to locate persons at-risk, assess and measure their risk level, characterise their personality and decision-making processes for managers and help analysts evaluate their organisation's vulnerability to insiders. These tools have included:

- The Insider Evaluation and Audit which takes managers through policies and practices designed to surface insider risk in employees through each step of the CPIR™ to allow them to assess their organisation's insider risk vulnerability. For example, the Audit uses Personal Predispositions to determine how well an organisation's screening and selection methods could detect such risks. It systematically reviews policies and practices designed to detect employee stressors or risk triggers, detect, and intervene in Concerning Behaviours without committing Problematic Organisational Responses, and detect emerging insider crime scripts. We frequently use the Risk Audit to demonstrate how an insider or group of insiders penetrated the different layers of organisational risk detection and management protections, revealing weaknesses.
- The Pathfinder™ application operationalises the CPIR™ as an analyst risk database, directing analyst information search using the Pathway through a series of questions derived from each CPIR™ category. It uses a series of algorithms to produce an overall CPIR™ score, as well as a rating in each category, while comparing a subject to group and "known bad" scores. The application takes about two hours to score a new case, is sensitive to risk changes over time and has good interrater reliability.
- Based on colleague complaints that the Pathfinder™ application was too time-consuming, Lenzenweger and Shaw produced the CPIR-Index™, a simpler operationalisation of the CPIR™ designed to produce similar risk score estimates within 20 minutes. The Index correlates closely with the Pathfinder™ risk score. The CPIR-Index™ provides a handy field screening tool and a common language for concerned security personnel to communicate about a case.
- Cognition communications software is designed to locate individuals at-risk for insider acts from their communications by identifying signs of Disgruntlement. Disgruntlement, defined as levels of Anger, Blame and Victimisation significantly different than peers, has been found to differentiate unhappy employees from those that have demonstrated insider risk indicators. Based on this earlier work, Cognition's psycholinguistic algorithms also provide an assessment of other risk areas (substance abuse, violence risk, religious extremism, dehumanisation, suicide, etc.) as well as characterisation of an author's psychological state, personality, and decision-making preferences.

> **…malicious insider activities are not isolated but instead result from a series of events.**

While we never conceived of the CPIR™ as the definitive analytical approach to insider risk assessment, it has served as a useful heuristic for analysts and managers within insider risk programs. According to Mitre, the CPIR™ has *"benefited the insider threat community by motivating security analysts and law enforcement to consider the whole person, recognise risk factors beyond concerning behaviors, and realize that malicious insider activities are not isolated but instead result from a series of events."* The CPIR's™ utility may lie in its' ability to tell a story about the evolution of insider risk that makes sense to practitioners, produces testable research hypotheses, and remains consistent with the available empirical research on insider actions.

Dr Eric D. Shaw is a clinical psychologist and former intelligence officer who has spent the last 25 years performing consultations, training, assisting in investigations and conducting research on insider issues while helping organisations manage insider risk. He is the founder and CEO of Insider Risk Group.

> **The CPIR™ has contributed to the development of several tools designed to assist analysts to locate persons at-risk…**

PAUL MARTIN

TEN TOP TIPS ON INSIDER RISK

Paul Martin's textbook, *Insider Risk and Personnel Security* (Routledge, 2024), explores the nature and origins of the problem (insider risk) and the means of tackling it (personnel security). This article attempts to distil the complex issues into a set of ten simple principles.

We often think of security as protecting us from bad things in the world outside. But the worst risks can come from within. They stem from insiders – people who betray our trust – and they require a different sort of security response. Human behaviour lies at the heart of these risks, making them the most interesting of all security problems. Insiders have been found in every type and size of organisation, from small tech start-ups to multinational corporations and government departments.

1 IT CAN GET PHYSICAL

Despite the impression created in some academic literature, insiders do more than just compromise cyber security. Insiders can inflict harm in varied and imaginative ways, including physical sabotage and violence. For example, trusted insiders have assassinated political leaders and suicidal airline pilots have deliberately crashed planes, killing everyone on board. It remains a notable factoid that whereas many hundreds of people have been killed by insiders, no one has (yet) been killed as a direct consequence of a cyber attack, as far as we know.

2 BEWARE OF THE (UN)KNOWN UNKNOWNS

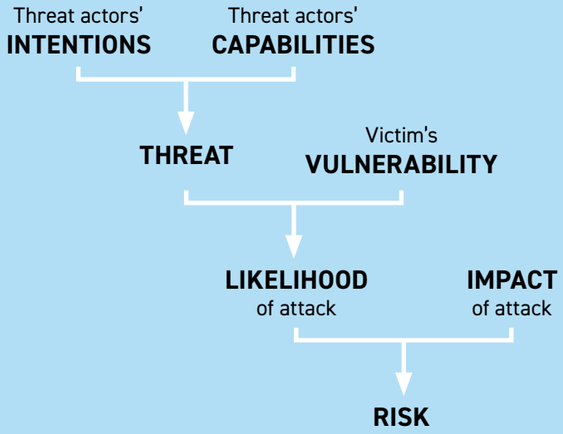
Insiders are capable of causing more harm than external threat actors because they already have legitimate access, know more about their victim, and may have authority over others. With the exception of the truly unwitting insider, they also behave covertly. The most capable insiders remain undiscovered for years and some may never be found. The history of espionage is littered with examples of enormously damaging spies who have operated in plain sight within high-security organisations for decades. The visible manifestations of insider risk are therefore only the tip of an iceberg of unknown size. This means, among other things, that the number of known insider cases within an organisation is a bad metric of insider risk. What it really measures is the ability to detect the problem. The absence of known cases is not evidence of absence of risk.

> **...the number of known insider cases within an organisation is a bad metric of insider risk.**

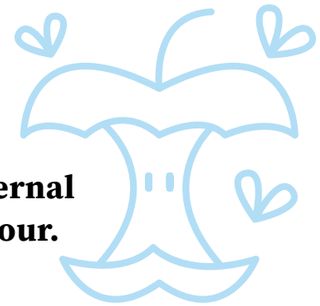
3 THE RISK IS DYNAMIC AND ADAPTIVE

In common with other types of security risk, insider risk is dynamic and adaptive: the risk changes over time and it adapts in response to the defensive actions of potential victims. Intentional insiders are intelligent threat actors who find ways of defeating security and remaining undetected. In some cases, their ability to do this is enhanced by support from a sophisticated external threat actor such as a hostile state agency. For personnel security to work effectively, it too must be dynamic and adaptive. This requires, among other things, agile mechanisms for discovering risks and genuinely learning lessons (as distinct from merely *identifying* lessons, which is all that many bureaucracies do).

The causal chain that generates insider risk and other security risks (Martin, 2019):



> **It falsely implies that insider risk is an inherent property of the individual, ignoring the crucial influence of work and home environments and other external factors in the genesis of insider behaviour.**



4 STRATEGY EATS CULTURE FOR BREAKFAST

Culture is important, of course. But a bigger barrier to effective personnel security in many organisations is a basic lack of strategic purpose. Personnel security should be an integrated system of complementary capabilities designed to achieve strategic outcomes like reducing risk, building trust and strengthening organisational resilience.

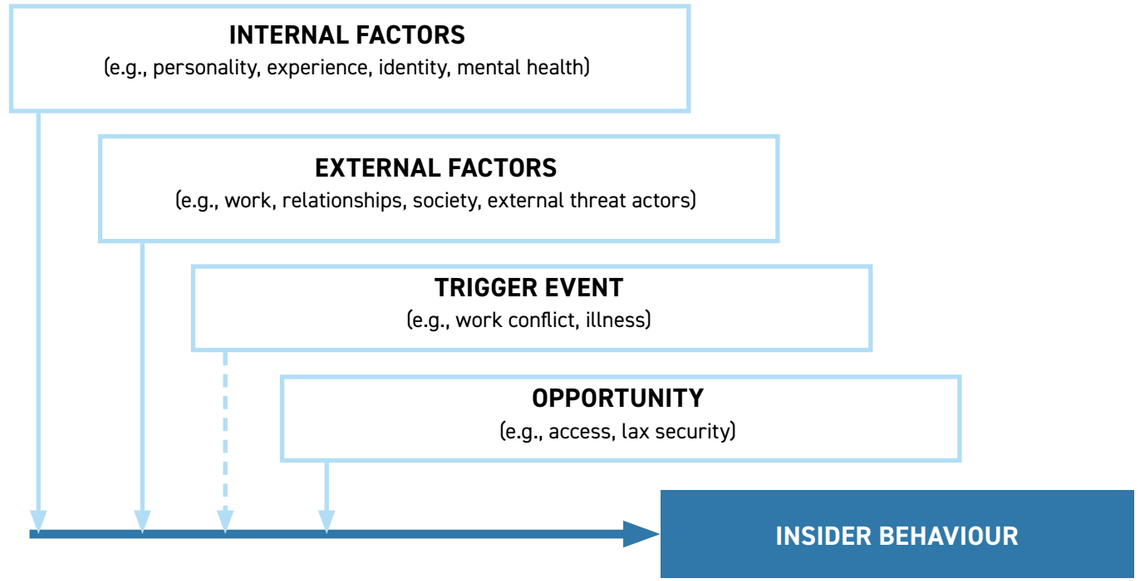
In practice, however, it is often a motley assortment of policies and processes that have accumulated over time, with little evidence base or strategic underpinning. Personnel security regimes that lack any explicit purpose or strategy tend to under-perform.

5 FORGET THE ROTTEN APPLES

Insiders are often portrayed as the few 'rotten apples' who lurk within an otherwise trustworthy workforce. The 'rotten apple' metaphor is deeply flawed, however. It falsely implies that insider risk is an inherent property of the individual, ignoring the crucial influence of work and home environments and other external factors in the genesis of insider behaviour.

It encourages a binary approach (trusted worker or rotten apple) to a risk that varies along a continuum. It also provides ammunition for marketeers who sell technologies that purportedly locate the 'rotten apples' through their behaviour on digital networks.

A simple model showing how internal factors, external factors, trigger events and opportunity combine in the development of insider behaviour (Martin, 2024):



6 PREVENTION IS BETTER THAN CURE

The ideal way to manage any security risk is to stop it from materialising, rather than waiting for bad things to happen and then dealing with the symptoms. The same is true for insider risk. Personnel security should aim to detect the weak early signals of potential insider risk and stop it developing into full-blown insider behaviour.

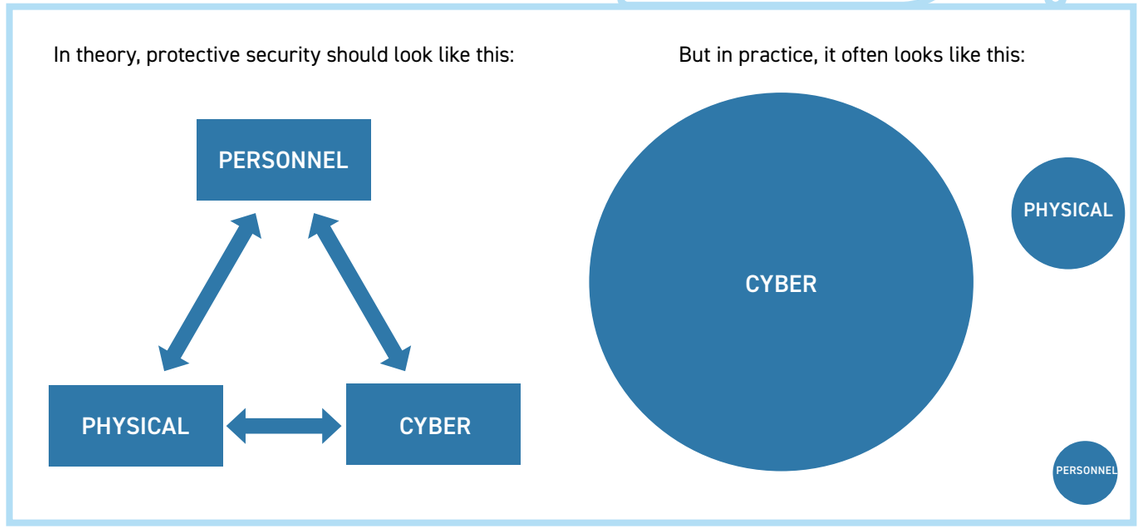
> **Personnel security should aim to detect the weak early signals of potential insider risk and stop it developing into full-blown insider behaviour.**

One way of doing this is through a welfare approach, in which the organisation seeks to help individuals with whatever problems might be nudging them onto the developmental path towards insider action. Most people are never going to become harmful insiders, and reaching for punitive action at the first sign of trouble is rarely the right answer.

7 RESPECT CINDERELLA

A central doctrine of protective security states that physical, personnel and cyber security are hugely interdependent and should therefore be managed holistically. A well-placed insider can defeat most physical or cyber security defences; cyber attacks can facilitate insider attacks; physical and personnel security measures are needed to protect cyber systems; and so on.

Nonetheless, many organisations have security structures that are far from holistic, with cyber security sitting in one silo and physical in another, while the personnel security Cinderella languishes homeless, or possibly with one foot in HR. Personnel security is also typically less well-resourced than its big siblings, and commands less attention at leadership level in many organisations.



> **Trust is the universal currency of insider risk and personnel security.**

8 IT'S ALL ABOUT TRUST

Trust is the universal currency of insider risk and personnel security. An insider can be defined as a person who betrays trust by behaving in potentially harmful ways: they have been trusted by an organisation, which gave them access to its assets, but they abuse that trust by behaving badly and potentially causing harm, whether intentionally or unwittingly. Arguably, the purpose of personnel security is to reduce insider risk and build trust by ensuring that people who have been trusted are trustworthy and remain trustworthy.

The four essential components of trustworthiness (after Martin, 2024):

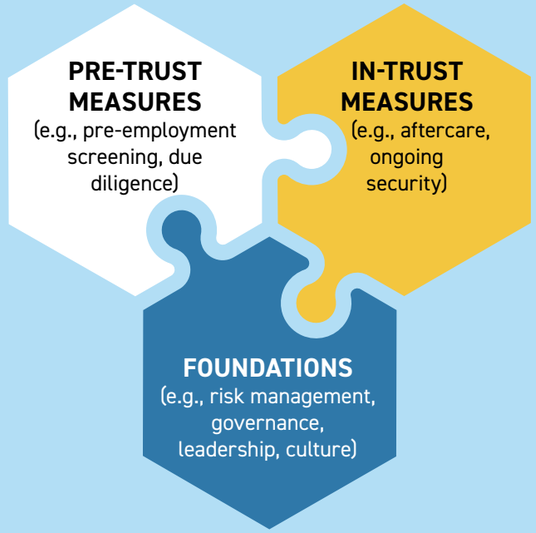
The components of trustworthiness	
BENIGN INTENTIONS	**INTEGRITY**
COMPETENCE	**CONSISTENCY**

9 THERE ARE NO SILVER BULLETS

It might be tempting to believe that a single process or piece of technology, such as an automated monitoring software package or pre-employment screening, can deal with insider risk. Tempting but wrong. Both in practice and in principle, no single process or technology by itself can ever be an adequate defence against insider risk. Personnel security requires defence in depth from a system of complementary measures.

The fundamental reason is that insider risk – in common with many non-trivial problems – is an emergent property of a complex adaptive system. Systems problems require systems solutions, not silver bullets.

A simple model of a personnel security system (Martin, 2024):



10 WORDS MATTER

Terms such as 'insider' and 'vetting' have many different definitions, creating ample scope for confusion. For instance, 'vetting' can be synonymous with personnel security in its broadest sense, or it may refer only to pre-employment screening. The two are very different. 'Insider' is also fraught with ambiguity. The previous CPNI definition ('a person who exploits, or has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes') meant that 'insiders' were the small minority of people who presented a heightened risk.

In contrast, the new (2023) NPSA definition classifies literally everyone with current or previous authorised access as an 'insider'. Both definitions are legitimate, but they have very different meanings. We should spell out what we mean when using these words.

Paul Martin CBE is Professor of Practice at Coventry University's new London-based Protective Security Lab and a Distinguished Fellow of RUSI. He has more than 30 years' experience as a practitioner in the national security arena. He is a former head of CPNI (now NPSA) and a former Director of Security for the UK Parliament.

JASON R. C. NURSE

COULD RANSOMWARE BE THE KEY TO BETTER CYBER DETERRENCE STRATEGIES?

This article is a call to action for policymakers, practitioners and academics to collaborate to deliver an effective ransomware deterrence strategy which could re-define cyber deterrence more widely.

Technological advances now touch every area of our lives. We work primarily at computers or on mobile devices, book medical appointments via apps, and even critical infrastructure like power and water stations are increasingly present online.

This connectivity benefits society incredibly but also opens us all to a diverse set of complex and persistent cyber threats. Even more distressing is the reality that many of these threats operate with impunity and are not deterred from their malicious online activities like their offline counterparts. Cybercriminals who perpetrate ransomware attacks are a perfect example but fortuitously they might also provide the key we need to better strategies for cyber deterrence.

WHAT IS CYBER DETERRENCE?

While the term cyber deterrence is relatively new, the concept and theory of deterrence has been around for a long time. The core idea is that a deterrence strategy aims to convince an adversary that the cost or penalty that they would encounter from conducting an attack is not worth any benefit that may materialise. Deterrence features in several domains (e.g., preventing crime) but is particularly studied at a nation state and political level, considering how states deter others from acts of aggression.

Cyber deterrence builds on this foundation and explores all facets of deterrence in cyberspace. One interpretation from Iasiello (2014) is:

> *"Cyber deterrence is a strategy by which a defending state seeks to maintain the status quo by signalling its intentions to deter hostile cyber activity by targeting and influencing an adversary's decision making apparatus to avoid engaging in destructive cyber activity for fear of a greater reprisal by the initial aggressor."*

This definition, albeit more politically oriented, highlights key components of deterrence online. Further to this conceptualisation, the author makes the case for at least two primary types of cyber deterrence. Deterrence by punishment where adversaries are dissuaded from attacks due to the reprisal actions (e.g., from those impacted or relevant authorities). And deterrence by denial – in this case the adversary is discouraged due to likely denial of the sought-after benefits.

In theory, this works well. A cybercriminal may be convinced not to hack into a bank because they may be caught, prosecuted, and imprisoned. Or, they may decide not to attempt the hack because they would face challenges transferring any ill-gotten funds to an untraceable account.

In practice however, this concept has not materialised as expected, and this is particularly visible in the case of ransomware attacks.

> **Ransomware poses a significant threat to business and states alike due to its indiscriminate nature and its ability to cripple systems.**

THE CASE OF RANSOMWARE

Ransomware is a malicious type of software that encrypts digital systems and prevents them from being accessed until a ransom is paid to an adversary. This form of cyber-attack has risen significantly of late with current statistics suggesting that 66% of organisations have been impacted and that ransomware payments totalled $1 billion in 2023. A unique facet of ransomware is also the link of some attackers to nation states, either as direct or indirect supporters.

Ransomware poses a significant threat to business and states alike due to its indiscriminate nature and its ability to cripple systems. We have witnessed attacks on government institutions (the Costa Rica government attack in 2022), local governments (Leicester City Council in 2024, City of Oakley, California in 2024, City of Augusta in 2023, Hackney Council, 2020, City of Atlanta in 2018), oil pipelines (Colonial Pipeline in 2021), health services (Change Healthcare in 2024, HSE in 2021, NHS in 2017), financial services (CNA Financial in 2021), food suppliers (JBS in 2021), and the education (British Library in 2023, Stanford University in 2023) and transport (San Diego Port in 2018) sectors.

These attacks have caused a range of significant harms to individuals but have also impacted the ability for countries to function effectively. In the case of Costa Rica in 2022, the attack was so damaging that the country declared a national state of emergency to deal with the crisis. At local government, the ransomware compromise of Hackney Council in 2020 meant that basic services such as social care and the land registry were unavailable. Worse yet, in 2023 the City of Dallas had its Police Department website knocked offline and other critical services like 911 were impacted.

The increase in ransomware attacks has been gradually matched by an increase in perpetrators and in sophistication of the ransomware ecosystem. To date, there have been countless ransomware groups, with some of the most prominent including LockBit, Conti, BlackCat/ALPHV, CLoP, REvil, Akira, Ryuk, DarkSide, Maze and Hive. Many of these groups function like legitimate businesses with management structures, HR departments and call centres.

Considering their significance and impact on society, a critical question is, what, if anything, has been done in terms of cyber deterrence?

RANSOMWARE AS AN OPPORTUNITY TO GET CYBER DETERRENCE RIGHT

Although cyber deterrence has been discussed in policy and academic arenas for decades, the reality is that there seems to be little agreement on how best to achieve it and how broad or narrow it should be regarded. This lack of clarity – and undoubtedly the international nature of the adversary – may well be key reasons why threats like ransomware have arisen.

Focusing first on what has been done to address the threat, there are a few poignant examples that align with traditional deterrence approaches. As it relates to deterrence by punishment, governments have sanctioned ransomware actors and law enforcement agencies have launched offensive cyber operations, takedown campaigns (as seen with Operation Cronos on LockBit in 2024) and arrested group members. There are also actions to deny ransomware groups financial benefits from their attacks. For instance, as a part of multinational collaborations, like the Counter Ransomware Initiative (CRI), in 2023 governments vowed not to pay or support ransom demands. Also of note is the growing ability to track and seize ransom payments, as was done in the case of Colonial Pipeline where at least $2.3 million in Bitcoin originally paid to the DarkSide group was seized by the US Justice Department.

> **Cyber deterrence strategies for ransomware – at least in the situations discussed – do not seem to be widely effective**

These strategies, albeit significant, seem to have had little prolonged, effective impact on deterring ransomware groups or their attacks. New ransomware operators and attacks continue to emerge. Even LockBit – which was itself the victim of a significant international law enforcement takedown operation – appears to have returned online only a few weeks later.

Arguably therefore, cyber deterrence strategies for ransomware – at least in the situations discussed – do not seem to be widely effective. Indeed, a recent UK National Security Strategy report stated:

> *"There is a high risk that the Government will face a catastrophic ransomware attack at any moment, and that its planning will be found lacking."*

While this lack of effectiveness is a critical issue, it also poses a tangible opportunity for academics, policymakers, and practitioners to join efforts to develop the field of cyber deterrence further – by focusing on a common enemy. Ransomware is a unique cyber threat that is not primarily perpetrated by nation states (albeit impacting them), is not bounded by physical properties (as traditional discussions around deterrence), requires international collaboration at various levels of government, law enforcement and private sectors, and is a policy as well as a technical concern. Defining an effective cyber deterrence strategy for ransomware could facilitate a more comprehensive understanding of deterrence in cyberspace in general, and provide the basis for future deterrence strategies.

Dr Jason R.C. Nurse is a Reader in Cyber Security at the University of Kent and an Associate Fellow at RUSI. His research focuses on cyber security policy, ransomware, and human aspects of security.

ZOE MARCHMENT

THE UNINTENDED CONSEQUENCES OF CRIME PREVENTION MEASURES

Few post-intervention evaluations on crime and security deterrence focus on the unintended consequences of that intervention. This article explores the existing evidence base on *crime displacement* and *benefit diffusion*.

Crime displacement

Criminal behaviour that is observed elsewhere or at different times because of that intervention.

Diffusion of benefit

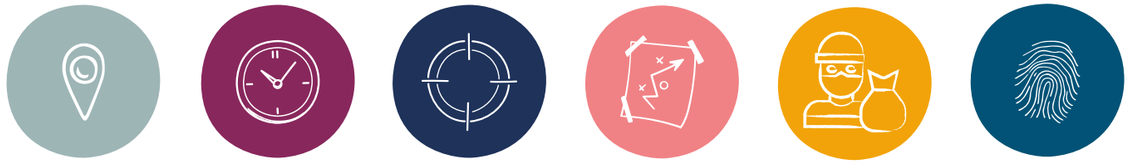
A reduction in crime among nearby locations and times that were not targeted by the intervention.

Our research identified and collated the existing evidence base for both displacement and diffusion of benefits following a crime deterrence intervention. We used a systematic approach to identify the relevant literature. The review considered peer reviewed studies that were published in English up to March 2021. The studies included an intervention designed to deter crime and at least one measure of deterrence.

DISPLACEMENT

We found 69 studies that attempted to measure whether displacement occurred after the introduction of one or more interventions designed to deter offenders from committing crime. Of those, 38 studies found indications of some form of displacement.

There are 6 types of displacement:



Spatial
A change in location

Temporal
Change of activity by the time of occurrence

Target
Crime against a different target

Tactical
The perpetrator adopts a separate modus operandi

Functional
A change in crime type

Perpetrator
When opportunities for a new type of offender occur

Spatial displacement was observed in 28 studies, half of which reported displacement effects through surveillance schemes, mainly formal police-based patrol interventions where perpetrators conducted criminal behaviour near the original target location. Closed-circuit television (CCTV) placement, the introduction of place-based lighting improvements, and target hardening efforts like gates and locks, all also reported displacement effects. Spatial displacement was also reported when interventions used a mixed measures approach to crime reduction.

The remaining displacement types were observed much less frequently. Temporal displacement was typically observed when perpetrators perceived surveillance and formal police-based foot patrol schemes as temporary and not a continual increase in security.

A diffusion of benefits is more likely to occur than displacement.

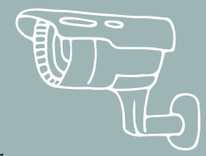
Only one study produced results indicative of target displacement after a residential property-marking scheme was introduced. Whilst the rate of burglary against residential properties decreased, there was an increase in commercial burglaries.

Tactical displacement was associated with target hardening in two studies that introduced burglary preventative measures like door-specific security upgrades. A study observing an increase in maritime guardianship/place management efforts also observed a change in piracy tactics.

Two studies found an associated functional displacement effect; one of which occurred after the introduction of burglary security devices. Crimes such as vehicle theft, theft from a person, robbery, and bicycle theft all increased.

Lastly, perpetrator displacement was identified in one study. After the introduction of various SCP (Situational Crime Prevention) and CPTED (Crime Prevention Through Environmental Design) measures at Rotterdam port, a shift in the perpetrator was seen. Port employees now became involved in cocaine trafficking. Employees typically either worked for port companies or government agencies and facilitated organised crime by bypassing security checks or providing information and/or access cards.

DIFFUSION OF BENEFITS



We found 33 studies that attempted to measure whether diffusion of benefits occurred after the introduction of one or more interventions designed to deter offenders from committing crime. 30 studies had findings indicative of a diffusion of benefits.

Formal surveillance-based interventions produced positive effects in three diffusion subtypes. Spatial diffusion of benefits was the most reported outcome across violent crime, theft, and burglary when introduced with police-based patrol schemes and increased guardianship/place manager interventions. Temporal diffusion was the next most reported benefit, mostly when introduced with marked vehicle and bicycle patrols. Lastly, outreach efforts saw a perpetrator diffusion effect when measuring gang-involved shootings in gangs not directly targeted by the intervention.

CCTV specific interventions contributed mostly to spatial diffusion of benefits across assault, robbery, burglary, and vehicle theft crime types. One study suggests that CCTV is dominant in providing a diffusion of benefits in more serious crimes compared to disorder types.

Target hardening schemes, such as implementing physical barriers, increasing access security measures, increasing the presence of uniformed officers at a location, and CPTED all had a spatial diffusion of benefits.

PRACTITIONER IMPLICATIONS

Despite the limited evidence base, we were able to extract useful insight for practitioners.

1. A diffusion of benefits is more likely to occur than displacement. 90.9% of studies that measured its presence found indicators of a diffusion of benefit. The corresponding figure for displacement studies was 55%.
2. A displacement effect is not indicative of a failed intervention. The focus should be on the level of harm produced by the intervention versus the level of harm prevented, which was underreported in the literature. For example, the volume of crime displaced may be lower than what was prevented in the treatment location, or the severity of the crimes could be less.
3. We know far less about temporal, target, tactical, functional, and perpetrator displacements compared to spatial displacement. This is an important gap to fill when studying crime types that are significantly motivated by target selection, tactics, and perpetrator specific recruitment strategies, like terrorism.

An important limitation of the existing evidence base is that not all studies in this topic are robust. Many employ quasi-experimental designs making it difficult to pinpoint whether the interventions were also responsible for the displacement/diffusion of benefit.

Dr Zoe Marchment is a postdoctoral research associate at University College London.

CHLOE SQUIRES

PROSECUTING FEMALE TERRORISTS: WHAT DO WE KNOW?

Research from Europe and America suggests women frequently receive lesser sentences for terrorism-related crimes than male offenders. What do we know about prosecuting female terrorists in England and Wales?

Existing UK based research suggests that female defendants tend to receive 33% shorter sentences than male defendants for terrorism related crimes (Monaghan et al., 2023). Exploring nuances within this overall average, this article analyses 546 terrorism cases (male n=503, female n=43) prosecuted in England and Wales between May 2006 and February 2024, and reveals a mixed picture. These figures relate to any terrorism related crime prosecuted in England and Wales, potentially capturing a mixture of returnees and non-travellers, though this remains unclear. While, on average women receive shorter sentences, on a case-by-case basis there is greater variability in sentencing for women prosecuted for terrorism offences, compared to male offenders. In this article, differences in sentencing and potential explanatory factors are discussed.

> **The dataset shows clear differences in the types of crimes men and women are prosecuted for.**

SENTENCING DIFFERENCES

The dataset shows clear differences in the types of crimes men and women are prosecuted for. With some exceptions, women were generally prosecuted for non-violent offences linked to providing support for terrorism.

Of the 19 offences shown in the data, women were prosecuted for just 9. Average sentences were generated across these offence types to understand whether there were differences in sentencing between men and women prosecuted for the same kind of crime. This resulted in 15 comparisons (Table 1).

In one case, male and female defendants received equal sentences. In 8 instances, the average female sentence ranged between 1.45 and 44 months shorter than the average male sentence. In 6 instances, the average female sentence ranged between 5 and 60 months longer than the average male sentence.

A direct comparison was possible between individual male and female cases in two instances (Table 2). In one case, the female defendant received a sentence 24 months shorter than the male defendant. In the second instance, the female defendant was given a life sentence 144 months longer than the male defendant.

Low numbers of comparable cases severely restrict the scope of this analysis. However, these findings indicate a wide variance in female sentencing which persist in comparisons between defendants prosecuted of the same offence. Overall, these differences in sentencing are not fully explained by differing offending behaviours and are yet to be fully accounted for.

WHAT MIGHT EXPLAIN DIFFERENCES IN TERRORISM SENTENCING?

Existing research may help explain this puzzle. A potentially useful argument to understand different legal responses to women associated with terrorism is that of gendered perceptions of agency. Hodwitz suggests, in the Balkans, women are prosecuted less frequently compared to men due to prevailing perceptions of women as 'victims' rather than perpetrators of terrorism, frequently 'excused entirely from criminal justice proceedings, bearing no more legal liability than children' (2022: 24).

Similarly, Counter-Terrorism Committee Executive Directorate (CTED) propose lenient sentences for women may be linked to '(often false) gendered assumptions about their limited agency' (2019: 2).

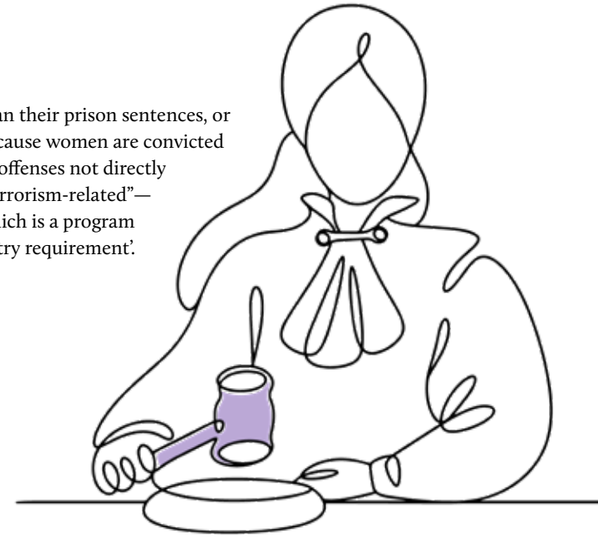
There are fewer explanations as to why women may receive heavier sentences than male defendants.

However, entrenched gender norms which expect women to be motherly and peaceful may facilitate 'greater shock value' (Krona & Caskey, 2023: 9) when women engage in terrorism, amplifying perceptions of danger, and potentially impacting sentencing.

Further possible explanations may be provided by structural criminal justice considerations. Factors such as a guilty plea, and the application of aggravating or mitigating factors have an important impact on sentencing. Beyond this, judges use guidelines to ensure that sentencing is fair and considers the different circumstances of offenders. The Equal Treatment Bench Book suggests that the impact of imprisonment is more acute on female offenders because many have neither a home nor a job to go to on release; are far more likely to be primary carers of children; and have usually committed a non-violent offence. Considering the different circumstances faced by women, The Female Offending Strategy suggests custodial sentences of less than 12-months should be avoided where possible, in favour of community sentencing. Ongoing analysis of sentencing remarks of 25 terrorism related cases (female n=9, mixed-sex co-defendants n=5, male n=11) seeks to find if these broader factors impact sentencing in terrorism cases.

POTENTIAL IMPLICATIONS

Existing research provides useful insight into the implications of shorter sentences for female terrorism offenders, suggesting they have an important impact on rehabilitation. Research based on interviews with practitioners in Europe suggested that shorter sentences for female offenders leave 'less time for in-prison rehabilitation and de-radicalisation measures'. Similarly, interview-based research with disengagement and radicalisation practitioners in the UK noted that, often, women cannot access prison-based programmes 'because the waiting period is longer than their prison sentences, or because women are convicted of offenses not directly "terrorism-related"—which is a program entry requirement'.



Implications of longer sentencing for women prosecuted with terrorism offences is yet to be fully considered.

DIRECTIONS FOR FUTURE RESEARCH

Sentencing is a complex process which accounts for different elements of the offence and the offender and further research is needed to explain the differences observed and isolate the factors causing this variation. Though this analysis is formed of a small data sample, further work in Europe and North America illustrates broadly similar sentencing trends. With existing research emphasising concerns short sentences for women may have on their rehabilitation, additional research is needed to understand and explore the potential implications this may have for wider criminal justice, counter terrorism, and deradicalisation measures.

Chloe Squires is a Doctoral researcher at the Handa Centre for the Study of Terrorism and Political Violence, University of St Andrews. Her interdisciplinary research focuses on women in terrorism and counter-terrorism, criminal justice, and legal responses to terrorism in England and Wales.

Table 1	Averages (months)		
Offence	**Male**	**Female**	**Difference***
Dissemination of a terrorist publication			
[2 counts]	40	45	+ 5
[3 counts]	64	20	- 44
[4 counts]	34.3	40.5	+ 6.2
[5 counts]	58	30	-28
Fundraising for the purposes of terrorism			
[1 count]	32.4	20.75	-11.65
[2 counts]	57	63	+ 6
[3 counts]	56	17	-39
Failing to provide information about acts of terrorism			
[1 count]	26.25	21	-5.25
Possessing/Collecting a record of information for terrorism			
[1 count]	36.5	17.5	-19
Belonging to, or membership of a proscribed organisation			
[1 count]	29.2	17.5	-11.7

Table 2	Direct comparisons (months)		
Offence	**Male**	**Female**	**Difference**
Engaging in conduct in preparation for acts of terrorism AND Dissemination of a terrorist publication	24	168	+ 144
Possessing/Collecting a record of information for terrorism [2 counts] AND preparation for acts of terrorism	120	96	-24

*NOTE: 'Difference' refers to the difference of female sentence compared to the male sentence.

'Count' refers to the number of charges for a single crime, i.e., committing the same crime numerous times.

Image credit: © *anna* | stock.adobe.com

DAVID MCILHATTON

EVALUATING SECURITY INTERVENTIONS FOR VENUES AND PUBLIC SPACES

The 'Evaluating Security Interventions in Public Locations' research project, responds to the challenge of understanding how best to evaluate protective security measures in an increasingly complex threat environment and across a significantly diverse range of venues and public spaces.

The project is based on four phases:

1. Assessing Protective Security Evaluative Practice;
2. Formulating Protective Security Logics for the Evaluation Design;
3. Evaluative Action Research in Use Cases; and
4. Adapting and Developing Evaluation Thinking Tools and Recommendations.

TOWARDS A THEORY OF CHANGE

The first phase was covered in a previous CREST article focused on a review of evaluation approaches within the extant literature base. In this article we focus on the development of protective security logics.

The objective of this phase was to formulate, through co-creation and dialogue, the change logic underlying protective security measures and interventions and to use this as a basis for meaningful evaluation. A Theory of Change approach was employed as a tried-and-tested method of bringing together a wide range of stakeholders to work together on a common set of tasks.

A Theory of Change is simply a logical way of demonstrating how interventions can be conceptualised and organised around the changes they create in relation to a particular issue. A good Theory of Change is an effective way of making the link between individual, everyday actions (or activities) such as 'holding an event' or 'installing CCTV cameras' to large, overarching goals such as 'reducing threat' or 'increasing resilience'. This approach begins with a problem or aim and works back in logical steps to the actions and interventions undertaken by individuals, organisations and partnerships. More specifically, it shows how activities lead to intermediate changes (outcomes) which then come together to tackle large-scale and often hard-to-measure problems (presented in the form of an aim).

> **There was a strong consensus across the groups that protective security is important in venues and public spaces.**

Crucially, it is an assumption-based model. It creates a set of theoretical causal links between the activities, outcomes and aim. These links are then tested through implementation and evaluation.

Researchers from Coventry University and Royal United Services Institute (RUSI) facilitated workshops with practitioners drawn from a wide range of backgrounds and with differing levels of experience and expertise in protective security and protecting venues and public spaces. Workshop participants included policymakers, law enforcement professionals and other emergency service representatives, faith-based organisation representatives, local authorities, security specialists and university staff from both academic and facilities backgrounds.

DEVELOPING PROTECTIVE SECURITY LOGICS

Posing to each workshop group the basic question "Why do we protect venues and public spaces?" and encouraging and prompting conversation led to a great amount of dialogue and introspection amongst practitioners. Some had a very clear idea as to why they do what they do based on previous negative experiences or specific threats which their groups face.

Often this was people with an obvious vocational commitment to their roles (e.g., a voluntary faith leader or law enforcement professional responsible daily for the safety of their respective publics). Others, including those more distanced from front-facing roles, were not able to answer immediately in great detail.

However, throughout the workshops, a common pattern emerged. There was a strong consensus across the groups that protective security is important in venues and public spaces in order to:

1. Protect life
2. Protect property
3. Protect the reputations of the location or those operating it
4. Ensure legal compliance
5. Enable people to live their life as they wish to freely go about their daily lives

These five principles enabled the development of a clear aim for protecting public spaces and venues. This aim was:

> *"To have safer and more secure venues and public spaces which provide people with the confidence to go about their lives and ways of life"*

This aim addresses the crux of protective security in that it directly seeks to improve the safety of venues and public spaces and those using them. It also goes a step further in aiming to provide those using venues and public spaces with the confidence and ability to go about their own way of life and to use a public space and venue as it was intended/as they wish.

This, for instance, means that places of worship must be able to remain open to worshippers who can use and access the premises in the way that they wish and that it was designed. It also means that people can use public transport or attend large venues with a high degree of confidence in their safety. Importantly too, through this, the aim also addresses concerns around the over-securitisation of venues and public spaces and negative, unintended consequences of protective security.

The workshops then identified two main objectives for achieving the aim:

1. People and places become more resilient and better able to respond to security threats and those using venues and public spaces have greater confidence in their safety and security.
2. Approaches to protective security become more standardised, joined-up, evidence-based, proportionate and able to demonstrate and justify their impact and value.

Broadly these represent the split in what it is that, from the perspective of practitioners, protective security interventions around venues and public spaces aims to achieve. On the left-hand side of the diagram (Figure 1) the three activity strands aim to make people and places safer, more resilient, and more confident. This, in many senses, represents the more visible outcomes. Whereas the right-hand side of the diagram aims to improve the practice, effectiveness and efficiency of protective security interventions around venues and public spaces – to influence and improve the sector. This, over time, represents a virtuous circle with one leading to improvement in the other.

During the workshops, many activities were discussed by participants. Though there was greater emphasis on some areas of work than others in different workshops, there was similarity in the content discussed by different stakeholder groups and across different areas. This suggests a high degree of commonality in understanding and practice around protecting venues and public spaces.

The Theory of Change diagram (see next page) makes sense of this diversity by using six groupings of activities, each of which is discussed below, using examples to illustrate the type and breadth of work undertaken and an explanation of the direct outcomes resulting from each type of activity.

The activities are not separated by partner, sector or job role. Rather this approach recognises that each element of the programme is likely to contribute to multiple types of activity. These activity groupings are:

- **Practical Physical Measures**
  This strand of work is often the most visible to the general public and is what many people, including practitioners, often think of first with protective security. It includes all forms of physical measures to protect including security guards, bollards and barriers. More complex facets of practical physical measures include the design and re-design of built environments.

- **Training and Capacity Building**
  This strand of work aims to raise the quality and quantity of capable protective security practitioners. This ranges from specialists in security to those who merely need to consider it as a part of a wider role (e.g., building managers, retail staff). It does this through training and development as well as encouraging legal compliance and the development and sharing of good practice in the sector.

- **Public Awareness Raising**
  This strand of work is one which aims to advise and educate the general public and users of venues and public spaces about threats and safety and security features. This includes media campaigns and signage, as well as educational products designed to raise peoples understanding and awareness of terrorism threat.

> **[the right-hand side of the diagram] over time, represents a virtuous circle with one leading to improvement in the other.**

- **Partnership and Collaboration**
  This strand of work covers many of the formalised aspects of partnership working which are not covered in the Training and Development or Research, Intelligence and Information Sharing Strands. Here areas of work such as sharing emergency planning protocols, impact planning and collaborating on specific events are kept distinct to represent the capacity and ways of working which exist in the sector and which enable effective cross-organisational and cross-sector working.

- **Research, Intelligence and Information Sharing**
  This strand of work includes both academic and non-academic research as well as advice and publications for practitioners and the general public. The work here is much of the formal knowledge on which protective security practice is based. Additionally, this strand of work also includes information sharing in established working groups and multi-agency fora which exist to promote data and intelligence sharing.

- **Strategy and Evaluation**
  This is a strand of work which is most often internally focused. It covers strategic planning, including the allocation of resources for protective security, and the evaluation and monitoring of work that is currently in place. Evaluation and monitoring are often both formative and summative, with some evaluation taking place in real-time and shaping planning and delivery and some taking place retrospectively.

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

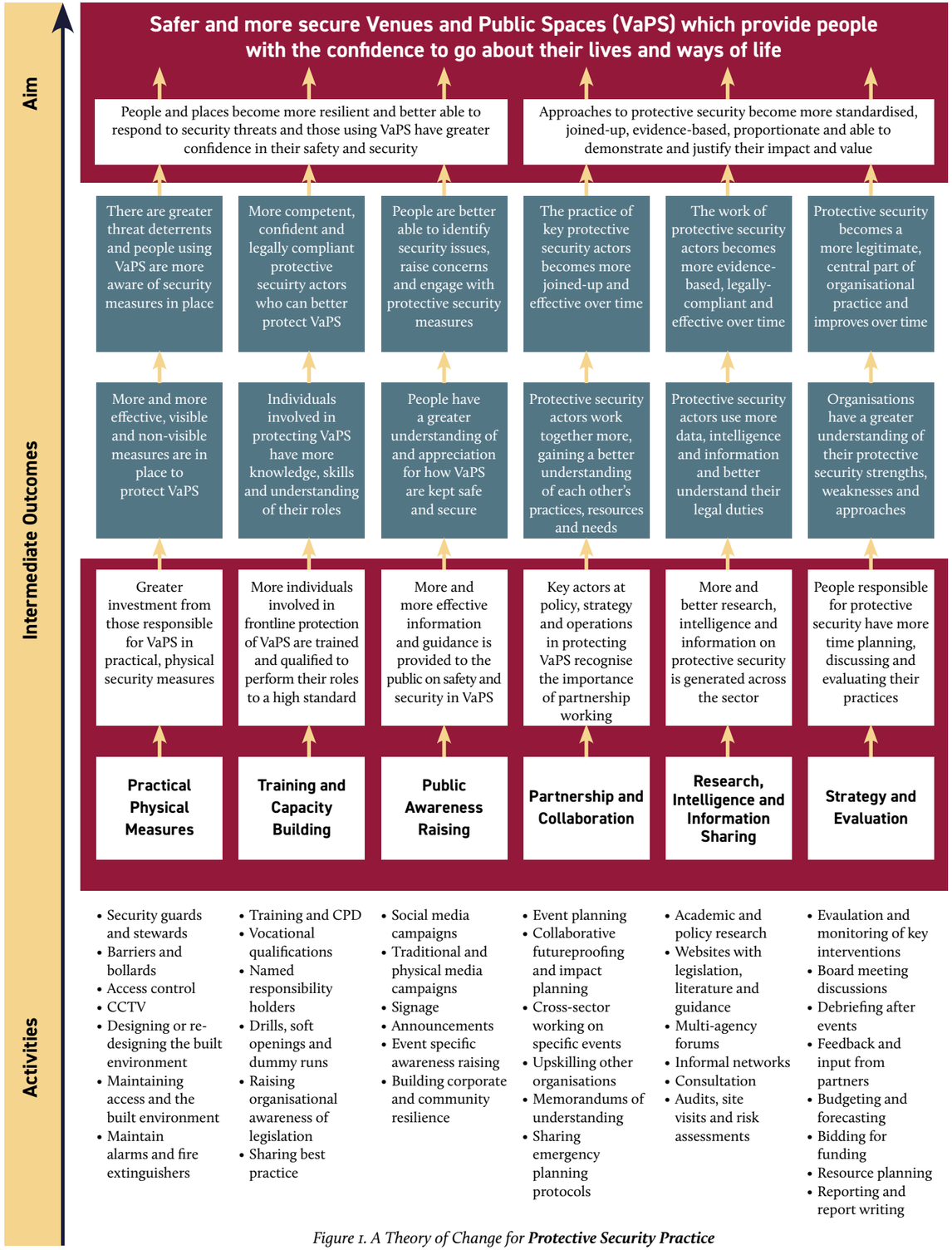


Figure 1. A Theory of Change for ***Protective Security Practice***

DON GRUBIN

RISK ASSESSMENT & POLYGRAPH TESTING

Around 20 years ago, some probation officers supervising sex offenders said they 'would quit if they no longer had access to polygraphy'. However academics were sceptical about the validity and effectiveness of the technique. Where do they stand now?

Police policy makers have typically been both cautions and suspicious about the use of polygraph testing, but in 2014 two police forces began to use polygraphy as part of their management of registered sex offenders. Since then another 12 forces have taken it on, and it has become possible to attach a polygraph condition to Conditional Cautions and Sexual Harm Prevention Orders. Nearly 3,500 individuals have now been tested, and approximately 5,000 tests have been carried out by police examiners.

Our data shows that over three quarters of these tests have resulted in previously unknown information being disclosed, sometimes leading to arrest, and nearly all have contributed to offender supervision. A recent independent review of police led management of sex offenders in the community recommended that polygraph testing in this setting should be made available to all forces.

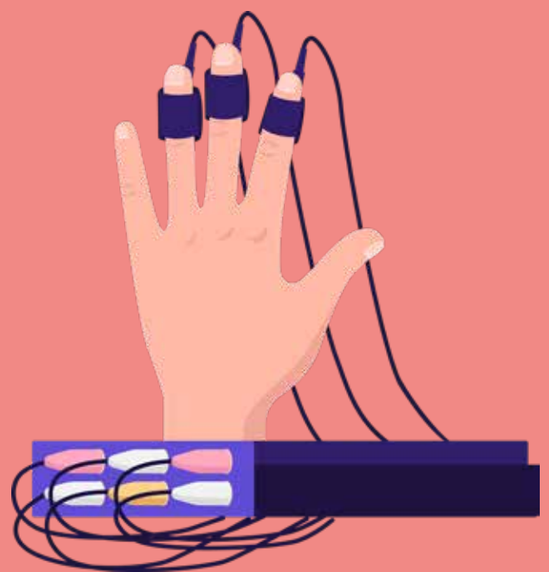
> **A polygraph test both obtains information and validates it.**

In view of the demonstrated contribution of polygraph testing to sex offender management it might be reasonable to ask about its potential for use in other contexts such as preemployment vetting, disciplinary proceedings, and Covert Human Intelligence Source (CHIS) oversight in order to not only detect problematic behaviour after it's happened, but also to help prevent it from occurring in the first place. To some this perhaps sounds too 'American' (although polygraph is in fact used in these types of setting in a number of countries), to others too controversial. Discussion, however, tends to be hampered by a misunderstanding of how polygraphy works and how it is, and can be used, not helped by the way in which it is portrayed in movies and on television.

POLYGRAPHY AND DECEPTION

Before even considering whether polygraph testing can or should have a role in policing beyond the management of sex offenders, however, a number of points need to be made:

First, although the polygraph is often called a 'lie detector', it doesn't detect lies. Instead, it records the physiological arousal associated with the cognitive processing required to lie, which involves memory, emotion, decision making, and inhibiting the default response of telling the truth, amongst other things. While cognitive arousal is of course not specific to lying, the way in which the polygraph examination is constructed aims to ensure that in this instance it is the deceptive response to a specific question that is the cause – this is achieved in a lengthy pre-test interview in which the salience of a small number of relevant questions is established which then become the focus of the test itself; the pre-test interview may take two hours or more while the testing phase lasts less than 15 minutes in total.



> **...although the polygraph is often called a 'lie detector', it doesn't detect lies.**

Second, while the polygraph is not 100% accurate in discerning deceptive from truthful responses, it performs much better than you or I can do on our own, with or without training (most studies find that training increases confidence but not accuracy) – best estimates are that a properly trained examiner using validated techniques is correct in 80 to 90% of cases compared with a 50 to 60% success rate for most individuals, even detectives (e.g., National Research Council, 2003). The 10 to 20% error rate, however, means that while the outcome of a polygraph test can be used to contribute to decision making, it is not relied upon on its own.

Third, there are two outputs from a polygraph examination, the test result itself (truthful or deceptive), and disclosures. They are complimentary to each other. A polygraph test both obtains information and validates it: since the start of police testing, disclosures of new information have been made in over 70% of tests with truthful outcomes, and in about 70% of tests following a deceptive outcome (although the latter are unlikely to be full disclosures, they open up useful lines of enquiry). Even without disclosures, however, the test result has meaning, with a truthful outcome providing reassurance and a deceptive one displaying a warning light that further investigation may be necessary.

Taking the above into account, the potential benefits of including polygraph testing in making decisions related to hiring, transfers into sensitive posts, disciplinary proceedings and accepting the account of a CHIS come into focus. Not only could it help avoid employing the wrong people or acting on incorrect information, but anecdotal evidence suggests that knowledge of an impending polygraph inhibits some inappropriate individuals from applying for posts in the first place, discourages those in post from engaging in problematic behaviour, and encourages honesty in CHIS (unfortunately this is not the type of matter that lends itself readily to a research study, and what data there is tends to be closely guarded by the agencies that hold it).

OBJECTIONS

What then are the objections? The main concerns appear to be that polygraph testing is intrusive, there is a risk of overreliance on its results, it can be beat, and it may be used in inappropriate ways.

While all these issues need attention, they can be mitigated by a well designed and implemented testing programme. The questions asked during a polygraph test are no more intrusive than those already being asked, the only difference being that the individual is put on notice regarding deception; all techniques used by the police have error rates, and it is not clear why polygraphy should be signalled out as the one whose results will override all other considerations (and there is nothing to indicate this is happening in sex offender testing); the polygraph can indeed be 'beat', but it takes practice to do so, and the few who might 'beat' it are already beating the system anyway, while many more who otherwise do so will be caught; and inappropriate use can be prevented by a proper quality control programme.

While the arguments for incorporating polygraph testing in a range of procedures beyond sex offender management are not cut and dried, there is now experience and data stretching over a number of years regarding the impact of polygraph testing in a police environment. There is also a considerable amount of evidence relating to polygraph testing of domestic abuse and terrorist offenders in addition to sex offenders by the probation service. Decisions about whether it should be put to wider use no longer need be based on what happens on daytime television.

Don Grubin is Emeritus Professor of Forensic Psychiatry, Newcastle University and (Hon) Consultant Forensic Psychiatrist, Cumbria, Northumberland, Tyne & Wear NHS Trust. He has many years' experience in the treatment and supervision of men who have committed sexual offences, and also has a longstanding research interest in this area.

PAUL THOMAS & MICHELE GROSSMAN

NEW INTERNATIONAL DIMENSIONS IN COMMUNITY REPORTING OF TERRORIST INVOLVEMENT

CREST research around community reporting of terrorist involvement by known 'intimates' has been replicated in North America and is now leading to an international policy-focussed research study.

The first people to suspect or know about someone becoming involved in radicalising to violence will often be those closest to them: their family, partners, close friends, or workmates. We've termed these 'social intimates' or 'intimate bystanders'. Until recently, little has been known about what the blocks or barriers towards reporting their concerns to the authorities might be for intimate bystanders, or what information, guidance and support might enable such reporting.

Our 2017 CREST research study built on Grossman's ground-breaking Australian research to identify that intimate bystanders **would** be motivated to make the momentous decision to report an intimate out of care and concern for both the person radicalising and the broader community, but would also face significant barriers or dilemmas in reporting.

Our data showed such barriers may include a lack of awareness about where they could find information and guidance on what they may be noticing, fear of backlash from others, concern for their own safety and confidentiality, and a lack of knowledge or confidence about what would happen after making a report. These CREST research findings directly informed the development of the 'ACT Early' campaign and web-resource led by the UK's National Counter-Terrorism Police (NCTPHQ), which has gone from strength to strength since its launch in 2020.

NORTH AMERICAN RESEARCH STUDIES

Our Community Reporting Thresholds research has subsequently been replicated in the USA (funded by the US National Institute of Justice) and in Canada (funded by Public Safety Canada), using the same methodology with even larger respondent samples. Both these North American studies have reproduced and confirmed the core, consistent findings from the Australian and UK studies. These consistent findings across a four-country study series include the intimate bystander determination to report based on care and concern, the desire for education and information sources which the intimate bystander would want to first research, the likelihood of using a 'staged process' of seeking guidance and support from own family/ friends and from 'community insiders' before formally reporting, and substantial concerns about safety (both for self and the intimate) and confidentiality.

The US and Canadian studies, did, however, also produce distinct, contextual findings. For example, the American study contrasted significantly with the UK study (where the largely Muslim-background respondent sample were willing to report directly to police and preferred to do it through face-to-face mode) in the reluctance of many US respondents to report directly to law enforcement, reflecting significant national concerns there around police violence and racism, and how law enforcement would therefore respond to a report concerning a non-White intimate.

The Canadian study found respondents also willing to report their concerns but being greatly worried about whether reporting would expose themselves to legal risk and so wanting their own source of legal advice and support.

There were also national differences in relation to preferences for reporting mode: while Australian and UK respondents overwhelmingly preferred face to face reporting, either directly to law enforcement or through community-based intermediaries, US and Canadian study participants were more comfortable with telephone and (in the US) digital reporting channels.

NEW RESEARCH ON POLICY AND PRACTICE

These research findings have now led to a new synthesis study, funded by the US Department of Homeland Security, that seeks to inform the creation of nationally appropriate community reporting frameworks, resources and mechanisms in the US and Canada. This new study - *'Addressing the Know-Do Gap in Community Reporting for Terrorism and Targeted Violence Prevention'* - brings together the principal investigators from the four previous national Community Reporting Thresholds studies (Michele Grossman (Australia), Paul Thomas (UK), David Eisenman and Stevan Weine (USA) and Sara Thompson (Canada) with Professor John Horgan (USA)).

"These CREST research findings directly informed the development of the 'ACT Early' campaign and web-resource led by the UK's NCTPHQ.

This two-year, three-stage project involves in-depth analysis of the four previous national Community Reporting Thresholds research studies in Stage 1 to identify congruence of key themes and the nature of divergences within the key findings. Stage 2 will see qualitative investigation of seven diverse national case study programmes, all of which involve encouragement to intimate bystanders to report concerns around someone close involved in violent extremism to the authorities.

This set of case studies involves two established initiatives directly informed by the Community Reporting Thresholds research – Act Early in the UK, and Step Together in New South Wales, Australia, alongside five other initiatives in Sweden, Denmark, The Netherlands, the US, and Canada. These case study programmes vary considerably - some are national, some are at state or regional level, some are owned and/or led by government or policing authorities and others by non-governmental organisations. Analysis and findings from these first two stages will inform Stage 3, a process of in-depth engagement with key policy stakeholders in the US and Canada to devise, develop and design systems and mechanisms to enhance community reporting of possible involvements in terrorism and targeted violence.

Paul Thomas is Professor of Youth and Policy at the School of Business, Education and Law in the University of Huddersfield. Michele Grossman is Professor and Research Chair in Diversity and Community Resilience, and Director of the Centre for Resilient and Inclusive Societies, at Deakin University's Alfred Deakin Institute in Melbourne.

TAYLOR CILKE & MARY ROWE

BYSTANDER REPORTING HELPS PREVENT MASS VIOLENCE

Bystander reporting's role in mitigating mass violence deserves much more attention – because peers, bystanders, and "bystanders of bystanders" often know a lot about a person's concerning behavior, and because they often choose not to report because they perceive authority figures are not receptive or are unlikely to be helpful.

Professionals in the field of threat assessment and management, which seeks to prevent mass attacks, have long agreed that bystanders are often key to preventing these acts of violence. Threat assessment and management professionals work quietly every day to prevent mass violence. This process involves the identification, assessment, and mitigation of threats. The identification piece is key – clearly, assessment and mitigation cannot occur before a threat is identified. Without – often heroic – bystanders who notice concerning behaviors and report them, becoming "upstanders," identifying threats would be a much more burdensome process for security practitioners and other authorities.

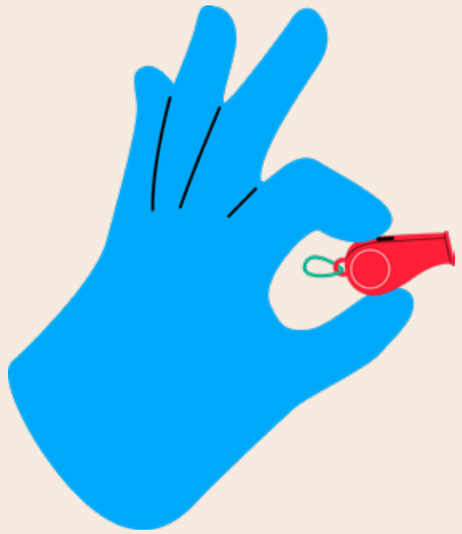
> **Security professionals cannot continue to call for bystanders to become upstanders without upholding our end of the bargain.**

However, security professionals cannot continue to call for bystanders to become upstanders without upholding our end of the bargain. While bystanders and security professionals have worked together to identify and mitigate significant threats throughout the years, cases like Lewiston, ME or Parkland, FL are reminders that more work is to be done.

The 2023 Initial Interim Report from The Independent Commission to Investigate the Facts of the Tragedy in Lewiston (the Commission) was a stark reminder of this. Initial findings appear to point out that the offender's teenage son, coworkers, brother, leadership, and others, identified that he was acting out of the norm and something needed to be done. The offender's concerning behaviors, which included paranoia, deteriorating mental wellness, and threats of violence, were noticed by those closest to him and those who worked beside him. On at least two occasions, bystanders made the heroic choice to report their concerns to law enforcement, and the Commission found several attempts by bystanders to address their concerns with the offender directly. Despite these efforts, on October 25, 2023, the offender killed 18 people and injured 13 others, before killing himself.

The tragedy in Lewiston, ME begs the question – why didn't authorities recognise the significance of the bystander reporting they received? This question may never be answered, but clearly the importance of the bystander reporting was not sufficiently recognised by authorities.

Research has found that bystanders are often hesitant to report their concerns for a wide variety of reasons. One very important reason is that they perceive the authorities who would receive their report to be unreceptive or unlikely to be helpful. Indirect bystanders, people who are bystanders-of-bystanders, may be hesitant for much the same, or entirely different reasons. These bystanders of bystanders are also vital to authority figures' efforts to prevent mass violence, as they often assist bystanders in the decision to come forward – or, unfortunately, discourage such action.



> **Bystanders often choose not to report because they perceive authority figures are not receptive or are unlikely to be helpful.**

It is essential that security professionals understand the people who report potential violence and understand the access to information these bystanders may have. A close family member in contact with a potential offender every day may hold different information than a spouse, a colleague, or an online stranger. Assessing the relationship that a bystander, or bystander of a bystander, has to the reported party may improve security professionals' ability to triage and respond to threats of violence.

Understanding the wide variety of barriers that bystanders face when considering reporting may also help security professionals triage and prioritise reports of concern. A tip from a concerned mother who thinks she has tried everything to prevent her son from violence and now feels she must go to law enforcement is different from a tip from a stranger about a post they saw online by someone they don't know; the stranger faces much lower barriers to reporting than the concerned parent. It is usually much more difficult for a close friend or family member to come forward, but once they overcome their barriers, their information often proves to be the most useful to authorities.

Ongoing education and awareness for security professionals and authorities in bystander reporting and barriers they face is imperative – and will contribute to preventing mass violence.

QUESTIONS FOR SECURITY PRACTITIONERS TO ASK THEMSELVES:

1. What relationship does this potential bystander have to the person about whom they are concerned?
   a. Are they a stranger, a friend, a family member, a peer, a coworker, an authority figure?
2. What is the context? Are they part of an organisation or community? What has happened recently?
3. Is this person a bystander of a bystander (an indirect bystander)?
4. Does this potential or actual source of information describe specific concerning behaviors they are worried about?
5. Does this bystander report having taken steps to address their concern? Have they spoken with the person directly? Have they contacted other authority figure(s) or other bystanders?
6. Have multiple potential bystanders reported concerns regarding the same person? If so, how has the organisation or community reacted? What steps have been taken thus far?

Taylor R. R. Cilke is a crime analyst at the Federal Bureau of Investigation's Behavioral Analysis Unit (BAU), Behavioral Threat Assessment Center. Her research focuses on the prevention of mass violence, bystanders, and the internet.

Mary Rowe is adjunct professor of Negotiation and Conflict Management at the MIT Sloan School, MIT, in Cambridge, Massachusetts. Her biography and publications can be found at https://mitmgmtfaculty.mit.edu/mrowe/research/

KATIE BENSON

DETERRING THE 'ENABLERS' OF ILLICIT FINANCE

A combination of approaches is needed to tackle the complex and multi-faceted problem of professional service providers enabling money laundering, corruption, sanctions evasion and other illicit finance related activities.

FROM 'MONEY LAUNDERING' TO 'ILLICIT FINANCE'

Since the 1990s, international bodies and national governments have raised concerns about the role that 'gatekeeper' professionals – such as lawyers, accountants, company formation agents, and real estate agents – can play in facilitating the entry of criminal proceeds into the legitimate financial system. This led to the expansion of global, regional and national anti-money laundering (AML) regimes, to include these sectors in the customer due diligence and suspicious activity reporting requirements that had previously only applied to financial institutions.

At the time, AML policy was primarily focused on the proceeds of drug trafficking and other organised crimes. However, a narrow focus on '(anti-)money laundering' does not address the range of crime and security threats of current concern and political prioritisation, which can be captured by the broader term 'illicit finance'. Illicit finance can refer both to funds generated from criminal or illicit activity, such as organised crime, corruption or tax evasion, and to funds used for illicit purposes, such as terrorism financing and proliferation financing.

Illicit finance is increasingly linked to the (inter)national security agenda, with, for example, the UK's Integrated Review of Security, Defence, Development and Foreign Policy explicitly recognising illicit finance as a national security threat in 2021, due to its role in 'financing malign actors' and the negative impact that the receipt of 'corrupt assets' has on the UK's global reputation. Russia's full-scale invasion of Ukraine in 2022 drew much-needed political attention to the global risks from kleptocracy and the role of the UK and others in providing a home to the wealth of corrupt elites. It also significantly increased the use of financial sanctions as a means of tackling illicit finance and achieving wider national security goals.

THE VARIED NATURE OF 'ENABLING'

Professional service providers can enable illicit finance in various ways. For example, accountants, lawyers and real estate agents can play a role, knowingly or unwittingly, in facilitating the laundering of organised crime or corruption proceeds through the purchase of property and other assets, managing front businesses, or moving funds through complex financial transactions and corporate structures. Trust and company service providers can establish and administer shell companies to facilitate tax evasion and help sanctioned individuals to hide their assets and thus limit the impact of financial sanctions. Lawyers, financial service providers, wealth managers, family offices and public relations agents are used by kleptocrats to both safeguard their assets and maintain or enhance their public profile and reputation.

> **...structural and systemic factors also play an important role and should be considered in strategies for prevention.**

However, enabling illicit finance is not just about individual actors; structural and systemic factors also play an important role and should be considered in strategies for prevention. For example, shell companies and other corporate vehicles – widely used in business and financial arrangements – can be misused to provide distance between illicit assets and their beneficial owners, hinder financial investigation and circumvent sanctions. The UK's network of overseas jurisdictions provides financial secrecy, which can also be exploited for the purposes of managing illicit wealth. Systems that enable anonymity in real estate purchases can allow illicit wealth to be invested in property without transparent direct links to ownership.

> **Illicit finance is increasingly linked to the (inter)national security agenda.**

A MULTI-PRONGED STRATEGY

The complexity of the threat from illicit finance, and the various professional services and systemic factors that can enable it, mean that no single approach will be sufficient for preventing or reducing it.

- Regulatory frameworks must be comprehensive and up-to-date, covering identified loopholes and jurisdictional asymmetries. They must also take account of the professional contexts and challenges of those working under them.
- Compliance with regulatory obligations and criminal laws should be promoted through measures to enhance the means and motivation for professionals to comply, alongside meaningful and appropriate enforcement.
- Enforcement requires successful detection, investigation, criminal/regulatory prosecution, and appropriate sanctioning. The UK has recently launched its first 'Professional Enablers Strategy', which aims to improve compliance and develop measures to better prevent and detect enabling activity through collaboration between regulators and law enforcement.
- Further understanding is needed of how the systemic features of the global financial system and the structural aspects of various professional service sectors enable different forms of illicit finance related activity - and political will is required to address them.

Dr Katie Benson is Lecturer in Criminology and Programme Director for the MSc Financial Crime and Compliance in Digital Societies at the University of Manchester, and Associate Fellow at the RUSI Centre for Finance and Security. She previously worked in roles in UK law enforcement. Katie's research focuses on financial crime, (anti-)money laundering, organisational misconduct, regulation and compliance.

Image credit: © *zgphotography* | stock.adobe.com

ALLYSA CZERWINSKY

LONELY BOYS AND MISOGYNIST INCELDOM:

CONSIDERATIONS FOR PRACTITIONERS WHO ENCOUNTER BOYS AND MEN AT RISK OF MALE SUPREMACIST THINKING

A summary of findings from Allysa Czerwinsky's doctoral work, examining entry pathways into misogynist inceldom and subsequent considerations for practitioners who may encounter at-risk individuals.

Male supremacist ideologies are increasingly discussed and (re) produced within both online platforms and offline environments, spreading from fringe spaces to the mainstream and prompting concern for parents, practitioners, and policymakers alike. Informed by my research examining the entry stories of current, exiting, and former self-identified incels across three online forums, this article outlines key findings and considerations for practitioners who encounter boys and men who may be at risk of turning to male supremacist thinking.

EXCLUSION, MARGINALISATION, AND VICTIMHOOD

Social exclusion and marginalisation were common across entry stories, including experiences of bullying, ostracisation, and feeling disconnected from peers, particularly those with sexual or romantic experience. These were linked to perceived deficits in physical attractiveness and personality characteristics, with community members using language demonstrating negative self-perceptions and low self-esteem. Experiences of exclusion and marginalisation due to physical unattractiveness and social deficits contributed to a narrative of difference from peers and a sense of unjust victimhood, feelings that may motivate at-risk individuals to seek out alternative avenues for belonging.

NEGATIVE EXPERIENCES WITH WOMEN

Struggling with heterosexual dating was an important pull factor, with repeated rejections acting as a catalyst for seeking out and participating in male supremacist spaces. Rejection sensitivity may heighten negative feelings toward women, who are viewed as the cause of repeated failures in the dating realm. Self-identified incels also reported experiences with women outside of dating that pushed them towards male supremacist thinking, including bullying, strained relationships with female family members, and trauma (sexual abuse and emotional manipulation) from maternal figures. These experiences may foster misogynist and anti-feminist views before individuals encounter male supremacist communities, which are further confirmed and legitimised once entering these spaces.

SHARED STORIES AND GRIEVANCES

Seeing similar experiences discussed by other users was a key influence in choosing to adopt the incel label and join male supremacist online spaces. Shared experiences and similar grievances helped foster belonging for newcomers through acceptance and validation. Open discussion and shared stories were also attractive features for individuals who felt that talking about men's struggles, society's increasing focus on attractiveness in dating, and their negative experiences with women were taboo within mainstream social spaces both online and off. For at-risk individuals, seeing similar experiences of marginalisation and rejection openly discussed in online communities may foster a sense of belonging and acceptance, acting as a powerful draw to join male supremacist communities.

'TRUTHFUL' IDEOLOGIES AND ATTRACTIVE ALTERNATIVE BELIEF SYSTEMS

Within male supremacist spaces, ideologies are largely framed as truth by community members, who use misinterpreted scientific knowledge or statistics presented out of context as evidence to support misogynist ideas and concepts. The black pill philosophy, one of the guiding worldviews for misogynist incels, posits that society is structured around a binary hierarchy of attractiveness informed by racial and class dynamics which is responsible for incels' suffering. This worldview reframes experiences of exclusion and rejection as a fundamental part of the incel experience, blaming both women and other men for prior victimisation. For at-risk individuals, male supremacist ideologies may allow them to weaponise experiences of victimisation against outgroups, legitimising harmful language and, at times, offline violence. Importantly, these belief systems transfer blame outward, making them an attractive philosophy for individuals who may already feel unjustly victimised and hold negative self-perceptions.

INTERSECTIONS AND COMPLEXITIES

Additional identity factors contribute to experiences of inceldom, including race and neurodiversity. Misogynist incel spaces appealed to non-white and neurodiverse men, as shared experiences of racism, racial prejudice, and the devaluing of neurotypical traits in the dating sphere and wider society were shared by other non-white and neurodiverse users in forums. Similarly, male supremacist spaces often speak directly to prior experiences of racism encountered by minority members, using pseudoscientific concepts and misinterpreted studies to prove women are responsible for upholding a societal structure that devalues non-white men. Ideologies that are structured around rules and black-and-white thinking may be particularly attractive to neurodiverse boys and men, who might struggle to form connections with peers and succeed in the dating sphere.

COMBATTING MALE SUPREMACIST IDEOLOGIES: CONSIDERATIONS FOR PRACTICE

Self-identified incels' entry stories displayed shared factors that contributed to participating in male supremacist communities and adopting associated ideologies. For some, experiences of exclusion and marginalisation, repeated rejection and negative experiences with women, and finding belonging and shared grievances can act as important pull factors for involvement in male supremacist communities. Additionally, male supremacist ideologies may allow individuals to rationalise prior negative experiences through an alternative belief system underpinned by evidence-based misogyny and clear rules around in and out groups. Practitioners who encounter individuals at risk of male supremacist thinking may benefit from:

For at-risk individuals, male supremacist ideologies may allow them to weaponise experiences of victimisation against outgroups, legitimising harmful language and, at times, offline violence.

- Acknowledging and validating prior feelings of hurt and harm, while working to offer alternative interpretations of life events beyond male supremacist ideologies
- Working to counter evidence-based misogyny through debunking, counter-narratives, and alternative evidence
- Building resilience through bolstering self-esteem and establishing systems of alternative support and belonging, including mental healthcare and social networks
- Considering the intersections between wider identity factors (race, neurodiversity, among others) and male supremacist thinking, and incorporating these into interventions and means of support.

Allysa Czerwinsky is a final year PhD Candidate in Criminology at the University of Manchester. Her research explores male supremacist communities online, with a particular focus on how personal and ideological narratives influence users' entries into, participation in, and exits from misogynist incel forums.

KIRK LUTHER, JOSEPH EASTWOOD & BRENT SNOOK

ARTFUL INSIGHTS:
ENHANCING RECALL IN INVESTIGATIVE INTERVIEWS THROUGH SKETCHING

Investigative interviews are crucial for obtaining detailed and accurate information from witnesses and victims — information that is necessary for solving crimes and delivering justice.

Over the years, various techniques have been developed to enhance information elicitation from interviewees. One promising memory enhancing technique is the sketch procedure, which involves interviewees talking through a sketch of the details of an experienced event. Let's take a closer look at the effectiveness of sketching as an interviewing tool.

WHAT IS SKETCHING, AND WHAT DOES IT LOOK LIKE IN AN INTERVIEW CONTEXT?

Sketching involves the interviewee talking through a detailed sketch of the experienced event. Sketching involves two main, concurrent steps, whereby the interviewee:

i. draws the scene or elements of the event, and
ii. provides a verbal explanation of the sketch.

Sketching is based on the principle of encoding specificity, which suggests that recall is enhanced when the same cues present during the encoding of an event are present during recall. By externalising memory cues through sketching, sketching aids in mentally reconstructing the context of the event, thereby enhancing the accuracy and detail of the information recalled.

> **...sketching aids in mentally reconstructing the context of the event, thereby enhancing the accuracy and detail of the information recalled.**

Here is what some sample sketching instructions look like (Eastwood et al., 2019):

In a moment, I am going to ask you to tell me what you remember from [the event under investigation].

Before you begin, I am going to ask you to try something that can often help people to remember more about what they have experienced [give paper and pen].

What I would like you to do is to please draw a detailed sketch of what happened [during the event that you experienced].

I would like you to sketch as many details as you can about the event. Importantly, I would like you to describe to me each item/thing that you are drawing as you draw it.

Please keep in mind that your artistic abilities are not being judged at all, but this is simply a technique used to enhance memory.

When you are ready you can start

[pause to allow interviewee to complete sketch].

What I would like to do now is go over what you saw.

Please feel free to refer to your sketch when telling me about what happened.

When you are ready, please go ahead and tell me, in as much detail as possible, everything that you remember from the event.

[Wait to ensure sure they have finished recalling information and pause for two seconds].

What else do you remember about the event?

WHAT DOES THE RESEARCH SAY ABOUT THE EFFECTIVENESS OF SKETCHING?

Enhanced Interviewee Recall:

Across various studies, sketching consistently leads to more correct details being recalled without increasing the number of incorrect details. For example, Eastwood et al's participants who sketched during an interview recalled 22% more correct details than those who did not sketch. This increase was particularly notable for object and action details, suggesting that sketching may be especially helpful for remembering visual and procedural aspects of events.

Enhanced Interviewer Recall:

Sketching also helps interviewers better understand the information provided by interviewees. By allowing interviewees to visually represent the scene and describe it, interviewers gain a clearer, more comprehensive picture of the event. By allowing interviewees to visually represent the scene and describe it as they draw, interviewers gain a clearer, more comprehensive picture of the event, which in turn can enhance their memory of the account. Luther et al. found that interviewers who watched an eyewitness create a sketch while describing an event recalled more correct details, fewer incorrect details, and fewer confabulations than those who only listened to the eyewitness's verbal account. These findings suggest that sketching can be a valuable tool for improving the accuracy and completeness of information gathered during interviews.

Detecting Deception:

In addition to enhancing interviewee and interviewer recall, sketching can be a valuable tool for detecting deception. Truth tellers and lie tellers tend to provide different types and amounts of detail in their sketches and verbal accounts. For example, Deeb et al. found that truth tellers tend to include more complications (unexpected events or obstacles) in their narratives, as these are a natural part of real-life experiences. Truth tellers also tend to provide more verifiable details, such as specific locations or actions that can be corroborated. Lie tellers, on the other hand, often strive to keep their stories simple and avoid details that could be easily disproven.

In the context of sketching routes travelled, Deeb et al. found that self-generated sketches were particularly effective for detecting deception. Truth tellers provided more details and were more accurate in their sketches than lie tellers, who often struggled to fabricate plausible routes and landmarks. This finding suggests that asking interviewees to sketch a route from memory, without the aid of a map, can be a useful technique for assessing the veracity of their statements.

> **...interviewers who watched an eyewitness create a sketch while describing an event recalled more correct details, fewer incorrect details, and fewer confabulations than those who only listened to the eyewitness's verbal account.**

Application in Real-World Contexts:

The effectiveness of sketching has been demonstrated in both controlled experimental settings and more ecologically valid live interactions, suggesting its practical utility in real-world investigative interviews. Overall, sketching appears to be a fast, frugal, and effective tool for interviewers.

The converging evidence from the literature suggests that sketching is a highly effective technique that can be used in real-world investigative interviews. Incorporating sketching in your interview will help improve the accuracy and completeness of information obtained from interviewees and help you (as the interviewer) better understand the information you obtain, thereby enhancing the overall effectiveness of your interviews.

Kirk Luther is an Assistant Professor from Carleton University. Joseph Eastwood is an Associate Professor from Ontario Tech University. Brent Snook is a Professor from Memorial University. Their research endeavors to advance the field of investigative interviewing by evaluating established techniques and developing novel approaches to inform policy and practice enhancements.

READ MORE

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

KATIE BENSON: DETERRING THE 'ENABLERS' OF ILLICIT FINANCE

Benson, K. (2020). Lawyers and the Proceeds of Crime: The Facilitation of Money Laundering and its Control. Abingdon: Routledge. *https://bit.ly/4gnogEI*

Benson, K. & Bociga, D. (2024). Occupation, Organisation, Opportunity and Oversight: Law Firm Client Accounts and (Anti-)Money Laundering, *European Journal on Criminal Policy and Research*. *https://bit.ly/4doV32I*

Cooley, A., Heathershaw, J. and Sharman, J.C. (2018). Laundering Cash, Whitewashing Reputations, *Journal of Democracy*, 29(1): 39-53. *https://bit.ly/4glaFAL*

Gudzowska, J., Lockhart, E. & Keatinge, K. (2024). Disabling the Enablers of Sanctions Circumvention. RUSI Centre for Finance and Security. *https://bit.ly/4gs7UxJ*

Heathershaw, J. & Mayne, T, (2023). Explaining suspicious wealth: legal enablers, transnational kleptocracy, and the failure of the UK's Unexplained Wealth Orders, *Journal of International Relations and Development*, 26: 301-323. *https://bit.ly/470QtK2*

Lord, N., van Wingerde, K. & Campbell, L. (2018). Organising the Monies of Corporate Financial Crimes via Organisational Structures: Ostensible Legitimacy, Effective Anonymity, and Third-Party Facilitation, *Administrative Sciences*, 8(2): 17. *https://bit.ly/3Be7XNd*

Prelec, T. & Soares de Oliveira, R. (2023). Enabling African loots: tracking the laundering of Nigerian kleptocrats' ill-gotten gains in western financial centres, *Journal of International Relations and Development*, 26: 272-300. *https://bit.ly/3ZnJqPX*

Transparency International (2019). At Your Service: Investigating How UK Businesses and Institutions Help Corrupt Individuals and Regimes Launder Their Money and Reputations. *https://bit.ly/3ZjbR1u*

Transparency International (2023). Through the Keyhole: Emerging Insights from the UK's Register of Overseas Entities. *https://bit.ly/3TrRUlt*

Zavoli, I. & King, C. (2021). The Challenges of Implementing Anti-Money Laundering Regulation: An Empirical Analysis, *Modern Law Review*, 84(4): 740-771. *https://bit.ly/4e24LD9*

TAYLOR CILKE & MARY ROWE: BYSTANDER REPORTING HELPS PREVENT MASS VIOLENCE

Borum, R. & Rowe, M. (2021). The Importance of Bystanders in Threat Assessment and Management. Meloy, J.R. & Hoffman, J. (Eds.). International handbook of threat assessment (2nd ed.). (pp. 423 – 425). New York, NY: Oxford University Press. *https://bit.ly/47p5vjc*

Federal Bureau of Investigation. (2017). Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks. Washington, DC. *https://bit.ly/47n1bkp*

Fein, R., Vossekuil, B., & Holden, G. (1995). Threat assessment: An approach to prevent targeted violence (Publication NCJ 155000). Washington, DC: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice. *https://bit.ly/4dYtF6H*

Fein, R. A., & Vossekuil, B. (1999). Assassination in the United States: An operational study of recent assassins, attackers, and near-lethal approachers. *Journal of Forensic Sciences*, 44(2), 321-333. *https://bit.ly/3XmEet3*

Marjory Stoneman Douglas Public Safety Commission. (2019). Initial Report Submitted to the Governor, Speaker of the House of Representatives and Senate President. *https://bit.ly/4e16Teb*

Low, E. C., Scalora, M. J., Bulling, D. J., DeKraai, M. B., & Siddoway, K. R. (2024). Willingness to report in military workplace violence scenarios: Initial findings from the Marine Corps on the impact of rank and relationship to the person of concern. *Journal of Threat Assessment and Management*, 11(1), 19–31. *https://bit.ly/4gsbNTl*

Rowe, M. P. (2021). Bystanders: "See something, say something" is not enough." *Alternatives to the High Cost of Litigation*, 39 (10), 153-165. *https://bit.ly/3XpMxEz*

Rowe, M. (2018). Fostering Constructive Action by Peers and Bystanders in Organizations and Communities. *Negotiation Journal*, 34(2), 137-163. *https://bit.ly/3ZnNz6j*

ALLYSA CZERWINSKY: LONELY BOYS & MISOGYNIST INCELDOM: CONSIDERATIONS FOR PRACTITIONERS WHO ENCOUNTER BOYS AND MEN AT RISK OF MALE SUPREMACIST THINKING

Czerwinsky, A. (2024). Misogynist incels gone mainstream: A critical review of the current directions in incel-focused research. *Crime, Media, Culture*, 20(2), 196-217. *https://bit.ly/3XHKNYw*

DON GRUBIN: RISK ASSESSMENT AND POLYGRAPH TESTING

Creedon, M., (2022). Independent Review into the Police-led Management of Registered Sex Offenders in the Community: Executive Summary. *https://bit.ly/3ZjuCBZ*

Grubin, D. (2008). The case for polygraph testing of sex offenders. *Legal and Criminological Psychology*, 13:177-189. *https://bit.ly/3ML2ZKq*

National Research Council (2003). The polygraph and lie detection. Committee to Review the Scientific Evidence on the Polygraph. Washington DC: The National Academic Press. *https://bit.ly/4ekGdVF*

JASON R.C. NURSE: COULD RANSOMWARE BE THE KEY TO BETTER CYBER DETERRENCE STRATEGIES?

Iasiello, E. (2014). Is cyber deterrence an illusory course of action? Journal of Strategic Security, 7(1), 54-67. *bit.ly/3TrjzCS*

Mott, G., Turner, S., Nurse, J.R.C., MacColl, J., Sullivan, J., Cartwright, A., & Cartwright, E. (2023). Between a rock and a hard(ening) place: Cyber insurance in the ransomware era. *Computers & Security, Elsevier*. *https://bit.ly/3XriImL*

Pattnaik, N., Nurse, J.R.C., Turner, S., Mott, G., MacColl, J., Huesch, P., & Sullivan, J. (2023). *It's more than just money: the real-world harms from ransomware attacks*. In International Symposium on Human Aspects of Information Security and Assurance (pp. 261-274). Springer. *https://bit.ly/47sWyoP*

House of Commons et al. (2023). A hostage to fortune: ransomware and UK national security. *https://bit.ly/4encfAs*

MacColl, J., Hüsch, P., Mott, G., Sullivan, J., Nurse, J.R.C., Turner, S., & Pattnaik, N. (2024). Ransomware: Victim Insights on Harms to Individuals, Organisations and Society. RUSI. *https://bit.ly/3XscZNT*

KIRK LUTHER, JOSEPH EASTWOOD & BRENT SNOOK: ARTFUL INSIGHTS: ENHANCING RECALL IN INVESTIGATIVE INTERVIEWS THROUGH SKETCHING

Dando, C. J. (2013). Drawing to Remember: External support of older adults' eyewitness performance. *PloS One*, 8(7). *https://bit.ly/3TrTDar*

Deeb, H., Vrij, A., Leal, S., Fallon, M., Mann, S., Luther, K., & Granhag, P. A. (2022a). Mapping details to elicit information and cues to deceit: The effects of map richness. *The European Journal of Psychology Applied to Legal Context*, 14(1), 11-19. *https://bit.ly/47pRly5*

Deeb, H., Vrij, A., Leal, S., Fallon, M., Mann, S., Luther, K., & Granhag, P. A. (2022b). Sketching routes to elicit information and cues to deceit. *Applied Cognitive Psychology*, 36(5), 1049–1059. *https://bit.ly/3ZpfbYN*

Eastwood, J., Snook, B., & Luther, K. (2019). Establishing the most effective way to deliver the sketch procedure to enhance interviewee free recall. *Psychology, Crime & Law*, 25(5), 482–493. *https://bit.ly/470SSVc*

Eastwood, J., Snook, B., & Luther, K. (2018). Measuring the effectiveness of the sketch procedure for recalling details of a live interactive event. *Applied Cognitive Psychology*, 32(6), 747–754. *https://bit.ly/3Bc5fYy*

Luther, K., Snook, B., Eastwood, J., & Fisher, R. P. (2022). Sketching: The Effect of a Dual-Modality Technique on Recall performance. *Journal of Police and Criminal Psychology*, 38(2), 469–482. *https://bit.ly/3MLCqoy*

ZOE MARCHMENT: THE UNINTENDED CONSEQUENCES OF CRIME PREVENTION MEASURES

Marchment, Z., Bouhana, N., & Gill, P. (2018). Lone Actor Terrorists: A Residence-to-Crime Approach. *Terrorism and Political Violence*, 32(7), 1413–1438. *https://bit.ly/3BoiueZ*

Johnson, S.D., Guerette, R.T. & Bowers, K. (2014). Crime displacement: what we know, what we don't know, and what it means for crime reduction. *Journal of Experimental Criminology*, 10, 549–571. *https://bit.ly/3XIwLpF*

PAUL MARTIN: TEN TOP TIPS ON INSIDER RISK

Bunn, M. & Sagan, S. D. (2016). A Worst Practices Guide to Insider Threats. In Insider threats, ed. by M. Bunn & S. D. Sagan. Cornell University Press. *https://bit.ly/3XlKukR*

Martin, P. (2024). Insider risk and personnel security: an introduction. Routledge. *https://bit.ly/3XsdWFX*

Martin, P. (2019). The Rules of Security: Staying safe in a Risky World. Oxford University Press. *https://bit.ly/4d80Wen*

NPSA (2023). NPSA changes to insider risk definitions. *https://bit.ly/4755OKb*

DAVID MCILHATTON: EVALUATING SECURITY INTERVENTIONS FOR VENUES AND PUBLIC SPACES

Winterbotham, E., White, J., Wallner, C. & McIlhatton, D. (2023). Evaluation Approaches for the Protection of Venues and Public Spaces from Terrorism. CREST. *https://bit.ly/4eorlp4*

ERIC D. SHAW: FROM RESEARCH TO PRACTICE & BACK AGAIN: IMPLICATIONS OF THE CRITICAL PATHWAY TO INSIDER RISK FOR CURRENT PERSONNEL SECURITY PRACTICES

Baweja, J., McGrath, S., Burchett, D., & Jaros, S. (2019). An Evaluation of the Utility of Expanding Psychological Screening to Prevent Insider Attacks. OPA Report No. 2019-067, PERSEREC-TR-19-05. *https://bit.ly/3XssWTY*

Myers, C., & Trent, A. (2019). Operational psychology in insider threat. In M. A. Staal & S. C. Harvey (Eds.), Operational psychology: A new field to support national security and public safety (pp. 157–184). ABC-CLIO. *https://bit.ly/47y2j4L*

Shaw, E. D. (2006). The role of behavioural research and profiling in malicious cyber insider investigations. *Digital Investigation*, 3(1), 20–31. *https://bit.ly/3XITeTB*

Shaw, E. D., & Fischer, L. (2005). Ten tales of betrayal: An analysis of attacks on corporate infrastructure by information technology insiders, Volume One. Defense Personnel Security Research and Education Center. FOUO. *https://bit.ly/3B4rLCK*

Shaw, E. D., Fischer, L., & Rose, A. (2009). Insider Risk Evaluation and Audit (Technical Report 09-02). Defense Personnel Security Research and Education Center. *https://bit.ly/3MMDY1D*

Shaw, E. D., Payri, M., Cohn, M., & Shaw, I. (2013). How often is employee anger an insider risk I? Detecting and measuring negative sentiment versus insider risk in digital communications. *Journal of Digital Forensics, Security and Law*, 8, 39–71. *https://bit.ly/3zkU3bI*

Shaw, E. D., Payri, M., & Shaw, I. (2017). The use of communicated negative sentiment and victimization for locating authors at-risk for, or having committed, insider actions. *Digital Investigation*, 22, 142–146. *https://bit.ly/463iQ33*

Shaw, E. D., & Sellers, L. (2015). Application of the Critical-Path Method to evaluate insider risk. *Studies in Intelligence*, 59, 1–8. *https://bit.ly/3MJdL3T*

Shaw, E. D., & Stock, H. (2011). Behavioral risk indicators of malicious insider theft of intellectual property: Misreading the writing on the wall [White Paper]. Symantec Corporation. *https://bit.ly/3TpedYQ*

Veenstra, K. (2015). Loyalty, social identity, and insider threat. Report prepared for the Australian Criminal Intelligence Commission. *https://bit.ly/3z5NauU*

CHLOE SQUIRES: PROSECUTING FEMALE TERRORISTS. WHAT DO WE KNOW?

CTED. (2019). Gender Dimensions of the Response to Returning Foreign Terrorist Fighters. *https://bit.ly/3MHorjF*

Equal Treatment Bench Book, (2023). *https://bit.ly/3TsfHBK*

Female Offender Strategy Delivery Plan 2022 to 2025. (2023). Gov.uk. *https://bit.ly/4e3xBmo*

Hodwitz, O. (2022). Gender-disaggregated data: Regional Analyses of Criminal Justice Outcomes in Terrorism Prosecutions. *https://bit.ly/4d7QTpo*

Krona, M., & Caskey, O. (2023). The Gangster and the Bride: The Media Representation of Masculinity and Femininity in News Coverage of Jihadi Terrorists. Terrorism and Political Violence, 1-16. *https://bit.ly/47uB8YK*

Mehra, T., Renard, T., Herbach, M., Hecker, M., & Koller, S. (2024). Female Jihadis Facing Justice Comparing Approaches in Europe. *https://bit.ly/470PREs*

Monaghan, R., Slocombe, B., Cuddihy, J., & Gregg, N. (2023). Prosecuting Extremists in the UK: An Exploration of Charging, Prosecution, and Sentencing Outcomes. CREST. *https://bit.ly/4e1v9ga*

Schmidt, R. (2020). Duped: Examining Gender Stereotypes in Disengagement and Deradicalization Practices. Studies in Conflict & Terrorism, 45(11), 953-976. *https://bit.ly/4e1dyFm*

PAUL THOMAS & MICHELE GROSSMAN: NEW INTERNATIONAL DIMENSIONS IN COMMUNITY REPORTING OF TERRORIST INVOLVEMENT

Grossman, M. & Thomas, P. (2017). What are the Barriers to Reporting People Suspected of Violent Extremism? CREST. *https://bit.ly/3B3FMAK*

Grossman, M. & Thomas, P. (2020). Community Reporting on Terrorism: Bystanders Versus Social Intimates. CREST. *https://bit.ly/3MJHoSQ*

Thomas, P., Grossman, M., Christmann, K. & Miah, S. (2020). Community reporting on violent extremism by 'intimates': Emergent findings from international evidence. *Critical Studies on Terrorism*, 13(4), 638-659. *https://bit.ly/4elBRO1*

Eisenman, D. P., Weine, S., Thomas, P., Grossman, M., Porter, N., Shah, N. D., ... Fernandes, M. (2023). Obstacles and facilitators to intimate bystanders reporting violent extremism or targeted violence. *Critical Studies on Terrorism*, 16(4), 672–699. *https://bit.ly/47uOlR5*

Thompson, S., Grossman, M. & Thomas, P. (2023). Needs, rights, and systems: Increasing Canadian intimate bystander reporting on radicalizing to violence. *Terrorism and Political Violence*. *https://bit.ly/3ZkQOLR*

Action Counters Terrorism (ACT). *https://actearly.uk/*

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 to identify and produce social science that enhances their understanding of security threats and capacity to counter them. Its funding is administered by the Economic and Social Research Council (ESRC Award ES/V002775/1).

The design of the research, data analysis and interpretation are completed independently by the research[*er] [team] and should not be taken as representative of views held by those who fund CREST.

CREST has established a growing international network of over 200 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**