AUTUMN 2017 / ISSUE 06

CREST SECURITY REVIEW

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

CREST

Decision Making

RESPONDING TO ERRORS IN CRISIS NEGOTIATIONS AND SUSPECT INTERVIEWS – p24

ASSESSING THREATS OF VIOLENCE – WHY THE PROFESSIONALS DO IT BEST – p10

CYBER SECURITY DECISIONS – HOW DO YOU MAKE YOURS? – p6

CONTENTS

DECISION MAKING

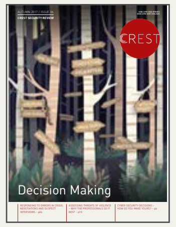
Highlights

MORE GULLIBLE THAN YOU THINK

We might think we wouldn't give our keys to a stranger, but most of us would - p22

DECISION MAKING UNDER STRESS

What factors affect the decision-making capability of groups in extreme or remote environments? – p4



CREST SECURITY REVIEW
Editor – Matthew Francis
Guest Editor – Paul Taylor
Illustrator – Becky Stevens
Designer – Steve Longdale

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

FROM THE EDITOR

On September 26th, 1983, Lieutenant Colonel Stanislav Petrov of the Soviet Red Army decided to do nothing. It was an incredibly important decision.

A new early-warning system had detected the launch of five American nuclear missiles. Petrov decided the report was an error, and that he would not ring his superiors to report a strike.

> Had he done so it was likely that his superiors, already primed to believe that the United States was planning to launch a first-strike, would have retaliated. The result would have been global nuclear war.

We all make thousands of decisions every day. Whilst thankfully most do not have the same kind of apocalyptic consequences, many are still critical to the security of the nation. From the x-ray operator at an airport to commanders at major incidents, these decisions can range from the mundane to the exceptional and urgent.

In this issue of *CREST Security Review* we highlight some of the latest academic research on decision making. As Julie Gore shows us in her article on page 14, there is a rich history of research on this topic. Nikki Power (page 8) looks at decision making during emergencies, and how the blue-light services work together. Laurence Alison, Michael Humann and Sara Waring draw on research in the same field, highlighting the importance of communication with casualties (page 18).

Emma Barrett and Nathan Smith's research looks at decision making under stress, and they give us some factors to help us assess a group's decision-making capability (page 4). Simon Ruda, from the Behavioural Insights Team, shows us how small manipulations can change the decisions made by large numbers of people (page 12), and if you're new to research on decision making we also have an A-Z guide to the key terms on page 28.

Drawing on recently published research, Jan-Willem Bullée (page 22) looks at how we can be manipulated into making bad decisions, and Renate Guerts, on page 10, shows us why professionals are needed to assess risks of violence.

> Of course, we don't always make the correct decisions, and on page 24 Miriam Oostinga draws on her research in interviews and crisis negotiations to show us how we can recover from different kinds of errors.

Drawing on the wider field of research on security threats, in this issue we have an article by Samantha Mann on how smugglers behave, on page 26, and understanding engagement in violent extremism, by Neil Ferguson on page 20.

This issue, on page 31, we've highlighted where you can read more about the research featured in the articles. Let us know if you find this useful. Our aim is to connect you, our reader, with research that has genuine impact and I'm keen to know if this way of signposting research is helpful to you or not.

Please let me know by emailing me at m.d.francis@lancaster.ac.uk

Matthew Francis
Editor, *CSR*

EMMA BARRETT AND NATHAN SMITH

DECISION MAKING UNDER STRESS

In 2014, 29-year-old Mohammed Uddin spent a few weeks with the Islamic State in Syria. On his return to the UK he was arrested and in 2016 convicted of preparing acts of terrorism.

The jury was told that Uddin returned to the UK because he couldn't tolerate conditions, which included hardships like cold water, poor food, 'stinky shared toilets', and the boredom of 'doing absolutely jack' (doing nothing). At one point, he told an associate back home 'U need to get used to the cold water and no electricity… It's tough bro lol, a LOT of patience is required'.

People who leave the relative comfort of developed countries to live in remote training camps or enter theatres of war often experience an abrupt and difficult transition. Not everyone can cope, as Uddin's case shows.

Remote and challenging environments are also encountered by security personnel who might be posted to them, for example, in critical infrastructure industries such as oil and gas organisations, as police or government liaison officers, as part of a military deployment, or perhaps undercover.

Studies of the performance of people who voluntarily enter extreme and unusual environments – mountaineers, polar explorers, astronauts, deep-sea divers, and cavers, for instance – highlight the ways in which decision making is affected by stress in challenging situations. These studies help us understand how decision making by terrorists and security personnel might be affected in similarly challenging environments, and highlight the implications for practitioners and policy makers.

The physical demands of extreme environments, such as severe temperatures, are often obvious and achieving goals can involve the risk of injury and death through, for example, suffocating, freezing, starving or falling.

Nasty as these are, physical hazards are not the hardest part of an extreme deployment. The psychological pressures can be as – or even more – challenging. It's not just the fear and anxiety triggered by ever-present danger. As Uddin's story illustrates, people in extremes also face days or weeks of monotony. And, the interpersonal pressures can become intolerable: being cooped up for weeks with the same small group of people raises the risk of destructive social conflict.

These physical and psychological sources of stress can interfere with decision making in many ways. Under acute (short-lived, high intensity) stress we focus on short-term rapid responses at the expense of complex thinking. This type of response can be life-saving when we need to react to immediate danger, but can also lead to 'tunnel vision' and ill-thought-through decisions.

In some cases, decision makers under stress experience 'decision inertia', a form of mental paralysis in which they procrastinate and find themselves unable to act.

Chronic, or enduring, stress can also have a corrosive effect. Experiencing danger, hardship, interpersonal pressure, sleep deprivation, and monotony for days at a time can lead to impaired vigilance, reduced stress-resiliency, suppressed emotion, and difficulties interacting with others. All in all, these responses are unlikely to promote sustained effective decision making.

Here are some factors to consider if you are assessing the decision-making capability of a friendly team or a hostile group.

1 WHAT IS THEIR 'INFORMATION ENVIRONMENT'?

Extreme environments can be characterised by uncertain, incomplete, ambiguous, and dynamic information. Circumstances in extreme environments can change quickly and unexpectedly. This makes it difficult to make an accurate assessment of the situation, thus interfering with good judgement and effective decision making.

2 HOW HIGH ARE THE STAKES?

Many decisions in extreme environments are inherently risky. Depending on the situation, correct navigation, choosing when to eat, where to sleep, and the type of equipment to use, can all mean the difference between success or failure. Under testing situations, decisions often need to be made in time-limited and dynamic scenarios. The stress of facing high stakes choices can lead to tunnel vision or decision inertia, and may induce perceived or actual time pressures.

3 WHAT IS THEIR PHYSICAL ENVIRONMENT?

Exposure to extremely hot or cold environments has been linked to slower reaction times, particularly when doing complicated tasks. At high altitudes, hypoxia (lack of oxygen) leads to mental confusion and slower decision making. Other physical aspects of the context often demand attention to stay alive. For example, in the deserts of North Africa and the Middle East, being alert to poisonous animals, incoming sandstorms, and sources of water could be the difference between life and death.

4 WHAT SOCIAL PRESSURE ARE DECISION MAKERS UNDER?

Being isolated with others can prompt destructive interpersonal conflict, even over little issues like snoring or eating habits. Being aware that colleagues are scrutinising decision making can be a significant and disruptive source of stress, particularly if you are concerned with what other people think of you. For instance, fear of appearing a coward may prompt an uncertain fighter to take reckless risks. Taking decisions as a team can also be problematic in high stress situations – too much agreement can end up with 'groupthink', and too much disagreement can result in indecisiveness, decision avoidance, or outright conflict.

5 ARE THERE PREVAILING CONDITIONS OF MONOTONY AND BOREDOM?

Not having enough to do can degrade morale, sometimes leading to petty squabbling, apathy, and depression. Sensory deprivation – monotonous landscapes, or constant droning noises – can also have strange effects, like hallucinations, and can have a serious impact on vigilance, and even mental health. All these, of course, interfere with the ability to make good choices in critical conditions.

6 HOW MUCH SLEEP ARE THEY GETTING?

Sleep deprivation, caused by lack of sleep or sleeping at odd times (as is common in a theatre of war, or in situations where personnel work shifts), can interfere with the ability to focus attention on relevant information, take in and process information, adapt to changing circumstances, and communicate effectively with team members.

How to make better decisions under stress

The research is clear: the best way to protect yourself from making poor decisions under stress is to train and prepare for it. Training enhances both skills and self-efficacy, enabling you to make better decisions and giving you the confidence to carry them out with minimal hesitation. High-pressure training simulations give you a taste of what it feels like to experience extreme stress and to understand your reactions to it. Practicing important physical skills repeatedly, like complex climbing manoeuvres, means they become 'over-learned' – engrained to a point of being automatic, and more likely to persist in the face of danger and fear.

Team preparation is important: a well-trained cohesive team acts in harmony, coordinating their actions and looking out for each other, to achieve complex goals in hazardous conditions. As part of preparation, consider what you and your team can do to maintain the most accurate information about changing physical conditions, perhaps via a 'base camp' crew that communicates with you effectively and often.

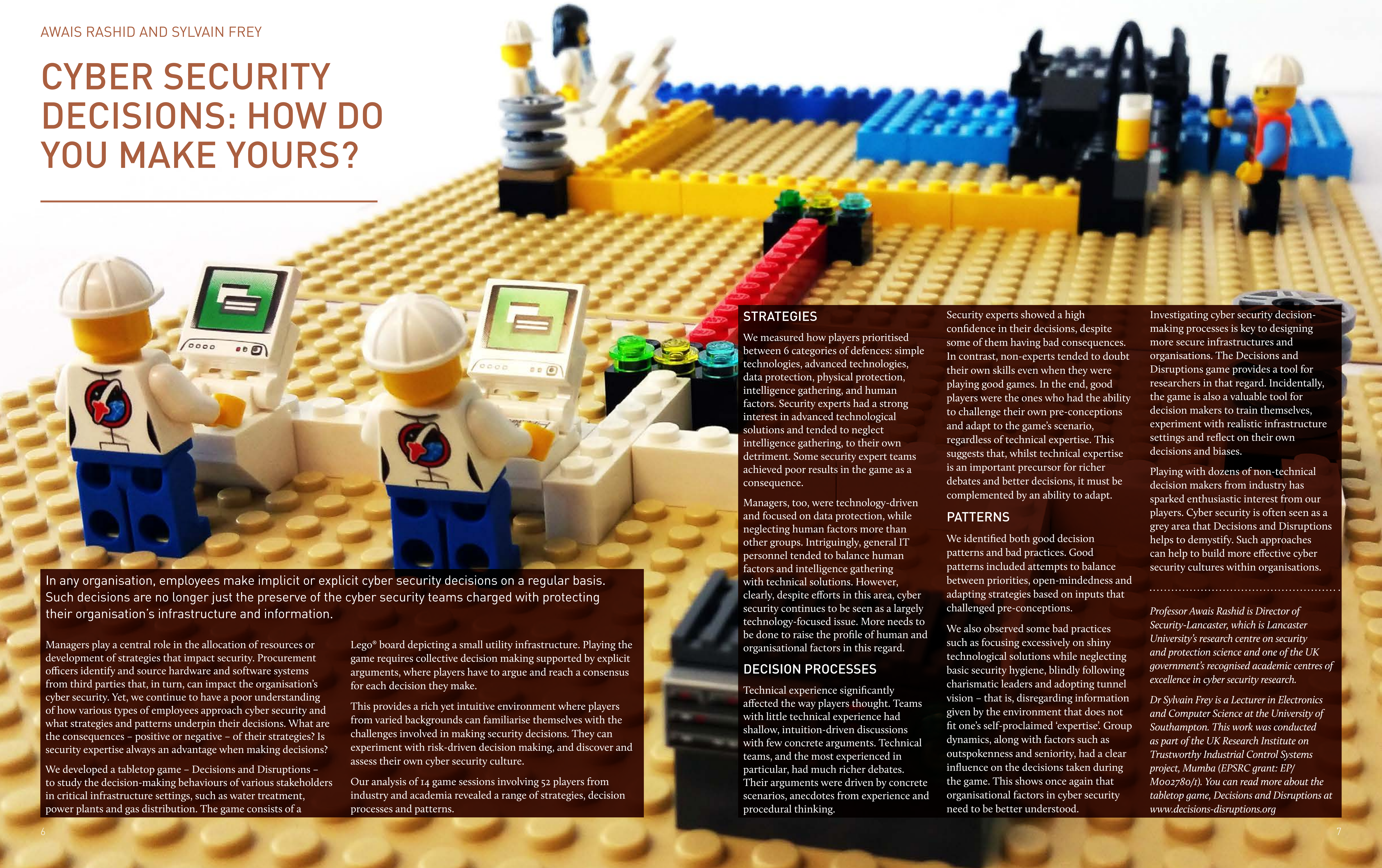
Once in an extreme environment, you can minimise the risks of social stress by keeping an eye on minor spats or simmering tensions that could escalate into something more serious, taking opportunities for privacy and 'time out' from the group, keeping busy – and most of all, being tolerant and tolerable.

Dr Emma Barrett is Research Fellow in Psychology at Lancaster University and CREST's Research to Practice Fellow. She is co-author of Extreme: Why Some People Thrive at the Limits *(OUP, 2014).*

Dr Nathan Smith is a Senior Research Scientist at Dstl and Honorary Lecturer at University of Exeter Medical School. He has conducted numerous studies with people in extreme environments.

AWAIS RASHID AND SYLVAIN FREY

CYBER SECURITY DECISIONS: HOW DO YOU MAKE YOURS?



In any organisation, employees make implicit or explicit cyber security decisions on a regular basis. Such decisions are no longer just the preserve of the cyber security teams charged with protecting their organisation's infrastructure and information.

Managers play a central role in the allocation of resources or development of strategies that impact security. Procurement officers identify and source hardware and software systems from third parties that, in turn, can impact the organisation's cyber security. Yet, we continue to have a poor understanding of how various types of employees approach cyber security and what strategies and patterns underpin their decisions. What are the consequences – positive or negative – of their strategies? Is security expertise always an advantage when making decisions?

We developed a tabletop game – Decisions and Disruptions – to study the decision-making behaviours of various stakeholders in critical infrastructure settings, such as water treatment, power plants and gas distribution. The game consists of a Lego® board depicting a small utility infrastructure. Playing the game requires collective decision making supported by explicit arguments, where players have to argue and reach a consensus for each decision they make.

This provides a rich yet intuitive environment where players from varied backgrounds can familiarise themselves with the challenges involved in making security decisions. They can experiment with risk-driven decision making, and discover and assess their own cyber security culture.

Our analysis of 14 game sessions involving 52 players from industry and academia revealed a range of strategies, decision processes and patterns.

STRATEGIES

We measured how players prioritised between 6 categories of defences: simple technologies, advanced technologies, data protection, physical protection, intelligence gathering, and human factors. Security experts had a strong interest in advanced technological solutions and tended to neglect intelligence gathering, to their own detriment. Some security expert teams achieved poor results in the game as a consequence.

Managers, too, were technology-driven and focused on data protection, while neglecting human factors more than other groups. Intriguingly, general IT personnel tended to balance human factors and intelligence gathering with technical solutions. However, clearly, despite efforts in this area, cyber security continues to be seen as a largely technology-focused issue. More needs to be done to raise the profile of human and organisational factors in this regard.

DECISION PROCESSES

Technical experience significantly affected the way players thought. Teams with little technical experience had shallow, intuition-driven discussions with few concrete arguments. Technical teams, and the most experienced in particular, had much richer debates. Their arguments were driven by concrete scenarios, anecdotes from experience and procedural thinking.

Security experts showed a high confidence in their decisions, despite some of them having bad consequences. In contrast, non-experts tended to doubt their own skills even when they were playing good games. In the end, good players were the ones who had the ability to challenge their own pre-conceptions and adapt to the game's scenario, regardless of technical expertise. This suggests that, whilst technical expertise is an important precursor for richer debates and better decisions, it must be complemented by an ability to adapt.

PATTERNS

We identified both good decision patterns and bad practices. Good patterns included attempts to balance between priorities, open-mindedness and adapting strategies based on inputs that challenged pre-conceptions.

We also observed some bad practices such as focusing excessively on shiny technological solutions while neglecting basic security hygiene, blindly following charismatic leaders and adopting tunnel vision – that is, disregarding information given by the environment that does not fit one's self-proclaimed 'expertise'. Group dynamics, along with factors such as outspokenness and seniority, had a clear influence on the decisions taken during the game. This shows once again that organisational factors in cyber security need to be better understood.

Investigating cyber security decision-making processes is key to designing more secure infrastructures and organisations. The Decisions and Disruptions game provides a tool for researchers in that regard. Incidentally, the game is also a valuable tool for decision makers to train themselves, experiment with realistic infrastructure settings and reflect on their own decisions and biases.

Playing with dozens of non-technical decision makers from industry has sparked enthusiastic interest from our players. Cyber security is often seen as a grey area that Decisions and Disruptions helps to demystify. Such approaches can help to build more effective cyber security cultures within organisations.

Professor Awais Rashid is Director of Security-Lancaster, which is Lancaster University's research centre on security and protection science and one of the UK government's recognised academic centres of excellence in cyber security research.

Dr Sylvain Frey is a Lecturer in Electronics and Computer Science at the University of Southampton. This work was conducted as part of the UK Research Institute on Trustworthy Industrial Control Systems project, Mumba (EPSRC grant: EP/M002780/1). You can read more about the tabletop game, Decisions and Disruptions at www.decisions-disruptions.org

NICOLA POWER

DECISION MAKING DURING EMERGENCIES: WHAT HAVE WE LEARNED AND WHERE DO WE GO FROM HERE?

People make hundreds of decisions all the time, ranging from everyday decisions with small, short-term consequences (e.g., what to have for breakfast?) to complex choices with large, long-lasting implications (e.g., which suspect to arrest for a crime?). The social sciences have long tried to help people make smarter and faster decisions. Recently these efforts have focused on improving decision making amongst emergency professionals.

Psychologists define decision making as the process of choosing an action to achieve a goal in an uncertain environment. When faced with a choice, individuals will gather information to develop their understanding of the situation, generate, evaluate and compare potential options, and commit to a decision by executing behaviour.

In predictable task environments, it is possible to engage in rational processing to optimise outcomes. Yet, decision making in the real-world is bound by cognitive and environmental constraints that make objective estimates difficult. A police officer responding to a major incident will have to juggle uncertainty about missing or conflicting information, manage high levels of risk, and cope with time pressure. It is the role of social science to explain how individuals make decisions in high-stakes and high-risk environments in order to develop and test novel interventions that might make the task easier, and the actions better.

What we have learnt about emergency decision making so far

Previous research has shown that decision making during emergency responses involves four phases: situation-assessment (SA; what is going on?), plan formulation (PF; what are my possible options?), plan execution (PE; how can I implement my plan?) and teamwork (T; who do I need to support my plan?). This 'SAFE-T model' provides a framework to support decision making, but the inherent ambiguity associated with emergencies can derail this process, causing decision inertia.

Uncertainty during emergencies can be endogenous and specific to the emergency itself (e.g., time pressure, lack of information) or exogenous and related to issues with the operating system (e.g., technology) and team (e.g., poor trust).

Research in this area has taken a largely exploratory approach to identify how responders cope with uncertainty, using a mixture of interviews and live/simulated training exercises. One study I was involved in coded the verbal communications used by police officers taking part in a live hostage negotiation training exercise. We found that police coped with uncertainty by adopting different uncertainty management strategies depending upon the SAFE-T phase; e.g., using reduction strategies (i.e., information search) to cope with uncertainty during Situation Assessment, or weighing pros and cons to deal with uncertainty during Plan Formulation. Our findings suggested that it would be useful to train responders in order to equip them with knowledge on which uncertainty management strategies to use during different decision phases.

In other research, we used a computer simulation of an airplane crash over a major city and found that inter-agency communications decreased in frequency when tasks were characterised by a lack of time pressure and poor strategic direction. These findings suggested that a clearer identification of goals and task deadlines could facilitate greater interoperability.

Although this research has provided important first steps to understand decision processing in real-world environments, there has been limited success in the testing and practical implementation of interventions to improve decision making. A possible reason for this implementation gap is due to the tendency for research to be exploratory. Research in this context has predominantly featured non-invasive observations of responders during training exercises, yet research must move beyond this stage to develop theoretical hypotheses around how behaviour might be influenced at the site of an incident.

A recent example of how research has been successfully translated into practice comes from the UK Fire and Rescue Service. Sabrina Cohen-Hatton and Rob Honey found that fire fighters tended to skip the Plan Formulation phase when making decisions at the incident. They recommended using 'decision controls' that encourage responders to think about the goal-directed outcome of their behaviour, suspecting that this might encourage more explicit plan formulation, which is important when evaluating actions in post-incident debriefs.

In a second study they tested their suspicion, finding that decision control training significantly increased plan formulation without delaying action. As a result, the UK Fire Service now use decision controls in operational practice. Thus, to have impact, empirical testing of recommendations from exploratory research must become an essential component to applied work.

The future of social science research in emergency response contexts

The increasing prevalence of security threats across the world has considerably increased our reliance on the Emergency Services. Although exploratory research will continue to play an important role in identifying challenges and developing potential solutions to emergency decision making, it is essential that future research goes beyond this stage to test and empirically validate solutions to support their implementation in the real-world. It is the responsibility of both parties to ensure that this relationship continues; bridging the implementation gap between research and practice via empirical validation and testing.

Dr Nicola Power is a lecturer in Psychology at Lancaster University.

RENATE GEURTS

WHY PROFESSIONALS ARE NEEDED TO ASSESS THREATS OF VIOLENCE

It could be argued that we are all threat assessors. Evolutionary instincts enabled our ancestors to recognise predators and, in modern society, similar instincts might tell us to avoid dark alleys or dense crowds.

Yet few of us would consider ourselves professional threat assessors. Although assessors have different backgrounds, from law-enforcement to psychology, they are charged with a similar task: To evaluate whether an individual who poses a threat of violence will indeed commit violence. Over the last 30 years, this task has developed into a profession. There are now associations for threat assessment professionals, conferences and training courses, and even a journal, the Journal of Threat Assessment and Management. But how do these developments pay off in practice? Does professional experience lead to better quality assessments?

To examine this question, we asked threat assessment professionals and laypersons to participate in a study in which they had to assess three fictitious cases. The cases reflected different domains of violence – domestic violence, public figure violence, and workplace violence – and described the context in which the threat evolved as well as the behaviours and characteristics of the person posing the threat. Participants had to assess the risk for violence in each case. Strikingly, the groups did not differ in their assessments. Professionals and laypersons had similar beliefs on what information signalled risk (e.g., prior violence, a communicated threat, experiencing loss) and what information mitigated risk (e.g., being liked by others, playing sports). One way of explaining this outcome is that intuition enables people to recognise danger when faced with it, regardless of professional experience. If this is the case, then why are professionals needed to assess threats of violence?

It turns out there are several reasons. One reason is that professionals, compared to laypersons, agree more with one another on their assessments. Clearly a conclusion about a case should depend on the information on that case, not on the person evaluating the case. Thus, agreement among professionals should be seen as a measure of quality. A second reason is that, when given the opportunity to request additional information to improve their assessment, professionals requested more relevant information. They sought to engage in a more comprehensive and less biased information search. This result fits well with theory and research showing that experts, whether they be chess grandmasters, physicians, or police officers, are particularly good at identifying critical cues in massive data. In other words, professionals know better what information to look for.

Interestingly, the latter finding suggests that if one would develop a checklist that summarises what information should be looked for, then laypersons would also be able to make accurate assessments. Part of this reasoning is probably correct. If laypersons were trained to use a checklist, their performance would most likely improve. However, evaluating potential danger includes more than simply listing risk factors as present or absent, because risk and protective factors interact with each other. Some factors only exist in combination with others, some factors outweigh or neutralise others, and some factors are so specific that they are only relevant in particular cases. The interplay between risk factors is not well understood yet on a scientific level, but its complexity underlines where algorithms fall short and expertise becomes necessary. The approach that draws on empirically informed guidelines, but relies on the discretion of a professional for the final judgement, is called Structured Professional Judgement and has been proven a reliable method for assessing risk of violence.

It is important for all parties involved with threats of violence to understand where threat assessment professionals may contribute most. Such an understanding enables the professionals themselves to manage the expectations placed on them. When stakes are high, professionals can face unrealistic demands to predict the future or draw firm conclusions based on little information. On the other side are those who consult threat assessment professionals, such as prosecutors, judges, or CEO's. Typically placed under time constraints, these officials need to invest their resources well and allocate expertise efficiently. Most critical, however, is that learning about threat assessment expertise could improve societal safety. Drawing incorrect inferences can be fatal when dealing with risks of violence, making it crucial to appoint the right person to the job.

The study described in this article is part of Geurt's doctoral thesis entitled Interviewing to assess and manage threats of violence *(September, 2017). Dr Geurts was a doctoral candidate in the House of Legal Psychology and affiliated with the universities of Gothenburg (Sweden) and Portsmouth (UK). From 2009-2014, Geurts served as a criminal investigator with the Dutch Police, and she is currently a board member of the Association of European Threat Assessment Professionals.*

SIMON RUDA

MEASURING DECISION MAKING

The Behavioural Insights Team is a company, jointly owned by the UK Government, which applies behavioural science to public services. Its Director of Home Affairs and International Programmes, Simon Ruda, writes about how their work can affect decision making by the general public.

Almost a century ago, early marketing theorists began to design surveys to try to understand what people wanted before selling it to them. On realising there were inconsistencies between what people said they wanted and how they actually behaved, psychologists and market researchers developed more advanced techniques to unpick motivations.

But even in-depth discussions are limited in providing accurate insights into decision making and behaviour. One of my favourite examples is a qualitative study into individual tax debtors, to understand why they failed to pay self-assessed tax. The focus-group based study confidently suggested that a sample of the general population would be more likely to pay when presented with information about how the taxes would be spent. However, the Behavioural Insights Team (BIT) then tested this hypothesis in the field using a randomised controlled trial (RCT) and found them no more likely to. The group who had expenditure explained to them did not show more willingness to pay than the group who did not get the explanation.

For the last few years, BIT have been encouraging governments, police forces and other agencies to routinely experiment as a means of measuring and improving the effectiveness of their operations. For this approach to be most efficient, it requires three principal elements. First, we should measure impact by observing actual behaviour, as opposed to self-reported behaviour or attitudinal measures. Where possible, routinely collected data (e.g., software updates) should be used as a measure of actual behaviour. Second, evaluations should create a counterfactual or 'business as usual' group – the experimentation element – against which a comparison can be made to determine impact. Third, there should be a willingness to add small adaptations or 'nudges' to key touchpoints, from letters to text messages to websites to face-to-face communication, with the aim of incrementally encouraging the desired decisions. There are important limitations to this approach, especially relating to crime and security. RCTs should be paired with other evaluation methods to ensure some outcomes are not missed. But in many other policy domains, such use of rapid, low cost, empirical field trials has significantly advanced our understanding of decision making, allowing us to develop more efficient services and more effective policies. We've seen this approach lead to hundreds of millions of pounds of tax debt advanced to the Treasury; a reduction in the over-prescription of antibiotics; increases in education attainment; reductions in racial disparities in Police recruitment, and many more, all at practically zero marginal cost.

THINK SMALL

The most important recent finding from this kind of public policy research has been the confirmation of Daniel Kahneman's hypothesis, that 'the environmental effects on behaviour are a lot stronger than most people expect'. That means that the small adaptations referred to above, if chosen correctly, can have disproportionately large impacts on human behaviour.

Since its inception, BIT has conducted in excess of 500 large-scale field trials that demonstrate this. But one of the most powerful examples relating to security comes from Carnegie Mellon. Experimenters found that participants in a study were more likely to divulge sensitive, personal information via an online survey when questions were phrased indirectly rather than directly. In a separate experiment, participants were more likely to divulge sensitive, personal information on a website that looked unprofessional, which the same participants rated as significantly less secure, than a professional looking website, which was rated as seeming more secure.

Environmental adaptations can have large impacts, but also unexpected ones. BIT recently partnered with a medium-sized police force to measure the impact, using an RCT, of body worn video cameras. In addition to positive justice related outcomes, we observed a reduction in the number of sick days taken by officers, yet no reduction in spells of sickness, suggesting the cameras had some effect on speeding up recovery times.

HUMANISING LAW ENFORCEMENT AND SECURITY REGIMES

Understanding how these environmental details affect decision making can, if harnessed effectively, be a powerful tool for policy makers and service deliverers to improve security outcomes. But we should primarily see built-in nudges as a way to optimise the systems and security regimes that serve our users and the population, and collect data that demonstrate how behaviour is being guided.

This approach to security is in its infancy. But one early observation is that security professionals tend to adopt an impersonal tone when dealing with the public, whether automated or face-to-face. To encourage decision making that is likely to support security concerns, we might consider a more human manner.

We recently partnered with West Midlands Police to increase compliance in one of the highest causes of harm in the UK: dangerous driving. We adapted the 'Notice of Intended Prosecution' – a letter sent to drivers caught speeding – to make it a bit more…well… 'human'. Rather than using legalistic language that only talked of sanctions, we explained how speeding limits were set and why drivers should comply with them.

We tested the impact of the revised sanction with an RCT, over a period of 6 months observing more than 15,000 drivers. The results were startling: a 13.7% increase in payment of the fine; a 41.3% reduction in those eligible for prosecution; and, most impressive of all, after another six months we observed a 21% reduction in future speeding offences in the West Midlands alone.

Further evidence to support the humanising of security-relevant, compliance-based interactions comes from procedural justice, a concept that promotes openness and fairness in processes over which users or the public have little agency. In Queensland, Australia, a procedural justice prompt for police officers conducting random breath tests increased compliance with their directives and improved levels of satisfaction, perceptions of police fairness and confidence in them.

In many aspects of security, multiple touchpoints exist with end users, the public, offenders, suspects, witnesses, victims or indeed actors within the system. Many of these touchpoints provide opportunities to test how small adaptations to business as usual can affect human responses, which cumulatively could have a significant effect on security. It's time we exploited them.

Read more about the research in this article at www.behaviouralinsights.co.uk/academic-publications

JULIE GORE, PAUL WARD AND GARETH CONWAY

NATURALISTIC DECISION MAKING AND UNCERTAINTY

Naturalistic Decision Making (NDM) addresses the cognitive problems and challenges associated with making decisions in demanding and uncertain situations.

NDM research emerged in the 1980s to study how people make decisions in complex real-world settings that are characterised by dynamic, uncertain, and rapidly changing conditions, and that require real-time decisions with significant consequences for mistakes. NDM methods emphasise descriptive studies conducted in field and operational workplace settings, complementing the controlled experimental studies that occur in the lab. It thus examines decision-making processes with the belief that, by examining what experienced people do cognitively well, research in this community can tap into this tacit knowledge – what experts implicitly 'know'.

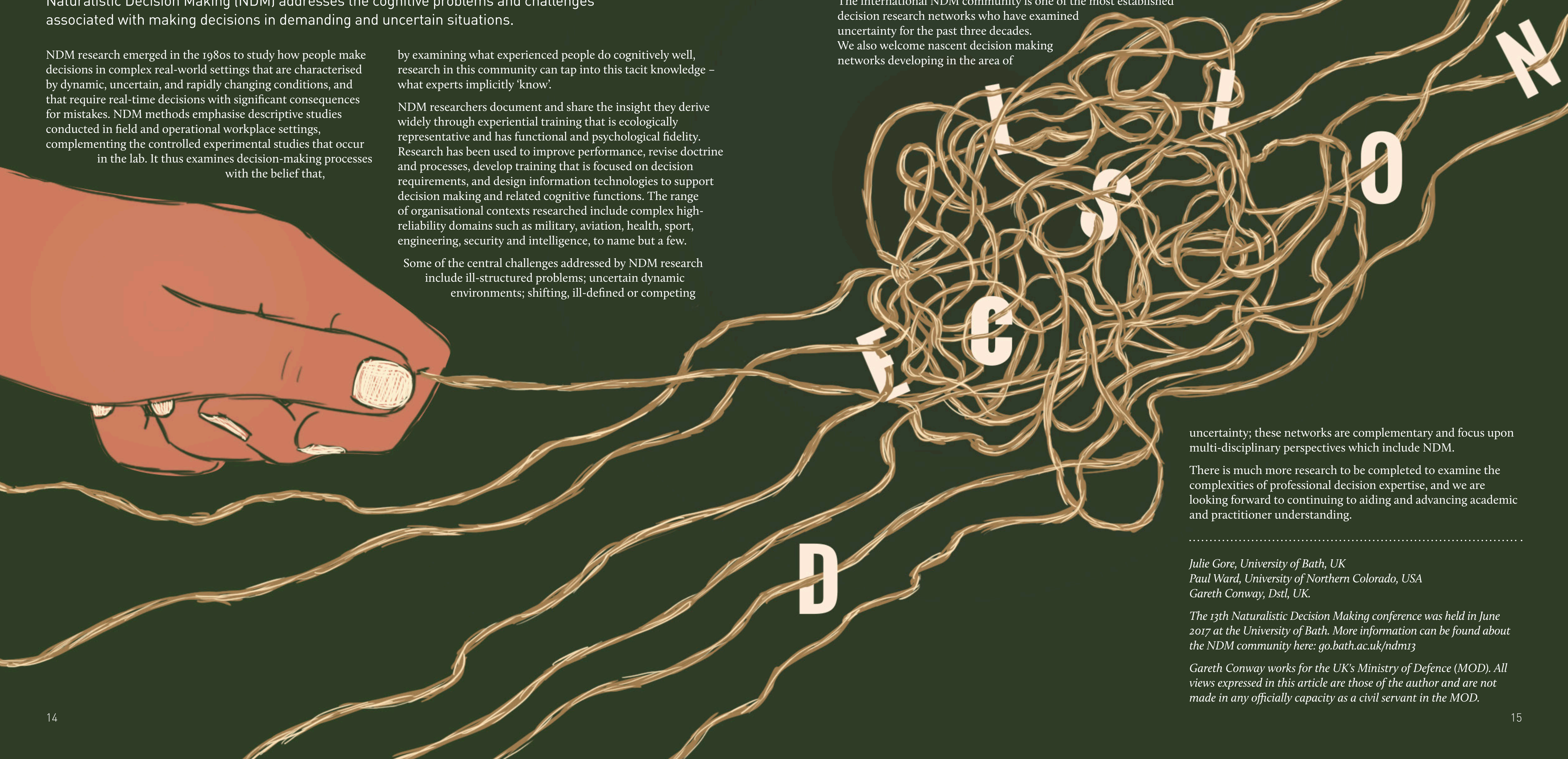
NDM researchers document and share the insight they derive widely through experiential training that is ecologically representative and has functional and psychological fidelity. Research has been used to improve performance, revise doctrine and processes, develop training that is focused on decision requirements, and design information technologies to support decision making and related cognitive functions. The range of organisational contexts researched include complex high-reliability domains such as military, aviation, health, sport, engineering, security and intelligence, to name but a few.

Some of the central challenges addressed by NDM research include ill-structured problems; uncertain dynamic environments; shifting, ill-defined or competing goals; action/feedback loops; time stress; high stakes; multiple players; and organisational goals and norms.

Research informed by NDM is currently aiding the criminal and intelligence services. Expert analysts tend to be people who have had decades of experience, often in diverse situations, which is consistent in expertise studies. While there has been considerable research in understanding the process of sense making in criminal intelligence analysis, there remain gaps in our understanding of how to move from documenting and eliciting sense making activities to the rigour of how arguments are constructed. Using cognitive task analysis methods developed by the NDM community, this work has outlined some of the considerations and strategies deployed during the analysis process, which can strengthen the analytical evidence base for practitioners.

The international NDM community is one of the most established decision research networks who have examined uncertainty for the past three decades. We also welcome nascent decision making networks developing in the area of uncertainty; these networks are complementary and focus upon multi-disciplinary perspectives which include NDM.

There is much more research to be completed to examine the complexities of professional decision expertise, and we are looking forward to continuing to aiding and advancing academic and practitioner understanding.



Julie Gore, University of Bath, UK
Paul Ward, University of Northern Colorado, USA
Gareth Conway, Dstl, UK.

The 13th Naturalistic Decision Making conference was held in June 2017 at the University of Bath. More information can be found about the NDM community here: go.bath.ac.uk/ndm13

Gareth Conway works for the UK's Ministry of Defence (MOD). All views expressed in this article are those of the author and are not made in any officially capacity as a civil servant in the MOD.

PAUL GILL

8 THINGS YOU NEED TO KNOW ABOUT TERRORIST DECISION MAKING

Terrorists from a wide array of ideological influences and organisational structures consider security and risk on a continuous and rational basis. Of course, the rationality of terrorism has been long observed. Traditionally, authors considered the rational adoption of terrorism as a strategy or a tactic.

More recently, and perhaps more interestingly, they have examined the kinds of rational decisions and behaviours that underpin the planning and commissioning of a terrorist attack.

Our recent research for a CREST-funded project on terrorist planning and decision making in the context of risk, led to us analyse over 80 terrorist autobiographies. Here are eight lessons from our study.

1 THE PROCESS OF ATTACK PLANNING VARIES WIDELY

On one end of the spectrum are accounts of attacks being 'more or less spontaneous' (Michael Baumann, former left-wing militant) and involving 'no great pre-planning… done in minutes' (Gerry Bradley, IRA soldier). On the other end of the spectrum are attack plans being drawn up over six months.

2 TERRORISTS CONDUCT COST-BENEFIT ANALYSES

In March 1988, Loyalist Michael Stone single-handedly attacked an Irish Republican funeral in Belfast with grenades and firearms. Stone hoped to 'take out the Sinn Fein and IRA leadership at the graveside'. Faced with thousands of mourners as well as policing and army units nearby, this was undoubtedly a highly risky attack. 'Most of the time it was 50:50. I figured [this attack] would be at least 60:40 against me, but could even be less'. Stone however felt the benefits were too great to pass up: 'I believed it was worth a risk if it meant the leadership of the Republican movement was wiped out.'

3 WHERE PLANNING IS INVOLVED, SEVERAL TARGETS ARE OFTEN CONSIDERED

Take for example Cathlyn Wilkerson's account of decision making in the Weathermen. 'When the proposal was floating about [targeting] Fort Dix, no one argued against it, but the tension in the air seemed to crystallize into a fine mist… As yet, however, we knew nothing concrete about the base, or exactly what we were talking about or whether it would be possible. We agreed to investigate other targets as well… One team went to each of the possible sites to do reconnaissance… [once completed]… the conversation focused on which of the targets we had investigated were feasible. Then we discussed the logistical details required for each action.'

4 SUBJECTIVE FACTORS PLAY A LARGE ROLE IN TERRORIST COST-BENEFIT ANALYSES

Many accounts of the planning phase note internal feelings of 'tension', 'stress', 'frayed nerves', 'doubt', 'frustration', 'paranoia', 'fear', 'inborn sense of danger', 'premonition of disaster', 'highly sensitised', 'hyper-aware', 'anxious', and 'scared'. Such feelings were also common during the commission of an attack. Attackers note physiological reactions like 'hand shaking', 'heart thumped like a drum', and an 'inability to sleep.'

5 OBJECTIVE SECURITY FEATURES PLAY A LARGE ROLE IN TERRORIST COST-BENEFIT ANALYSES

For example, Michael Stone's first assassination target was the Sinn Fein politician Owen Carron. Initially Stone surveilled Carron's home address: 'I knew he had two dogs… I knew that all over the house and garden he had the best security and surveillance equipment money could buy. He had cameras and sensors. He even had tin cans tied to a tripwire strung across the field at the back of his house to alert him to the security forces that watched his every move… I ruled out attacking him at his home because he had too much security and I could not get close enough to kill him without being spotted or killed myself. My best option was his constituency advice clinic… [it] was the weakest link in his daily routine.'

In many cases you could do it all yourself, it will just take a little more time. AND, without taking unacceptable risks. The conclusion is undeniable.

Anders Breivik on why to forego co-offenders.

The bank branch was chosen for its lack of adjacent buildings.

UK left-wing extremist group, Improvised Guerrilla Formation, claims responsibility for an incendiary device attack against a Bristol bank in 2013.

6 TERRORISTS EXPECT SECURITY FEATURES

They actively search for poor deployment of security. Eric Rudolph's reconnaissance of the Atlanta Olympics Park noted: 'Hundreds of security guards and cops patrolled the park. They eyeballed me going through the entrances. But there were no metal detectors, and bags were searched selectively. After sundown the crowds grew enormous… Security at the park became overwhelmed. They stopped searching bags altogether, and the entrances flew wide open. I knew then that I could smuggle in a bomb.'

7 PERCEPTIONS OF THE SECURITY EFFECTIVENESS MATTER MORE THAN THEIR SIMPLE DEPLOYMENT

For example, this was evident in Gerry Bradley's account of his PIRA activities. In particular, the use of helicopters in surveillance: 'The chopper destroyed us. If the chopper was up, you weren't allowed to move out of a house… Ops were cancelled regularly because of it. They could read newspaper over your shoulder from the chopper.'

8 PERCEPTIONS OF RISK SHIFT WITH EXPERIENCE

The experience of not being caught for previous crimes leads offenders to downplay the immediate situational risks of their current activity. The same is true for terrorists, as Ann Hansen, a former anarchist noted: 'A steady diet of small illegal activities had boosted my confidence in our abilities to get away with things. I no longer imagined a cop hiding behind every obstacle and actually found myself feeling quite relaxed out on a mission.'

Paul Gill is a Senior Lecturer in Security and Crime Science at University College London. He led a CREST- funded research project focusing on terrorists' decision making. You can read more about the project here: www.crestresearch.ac.uk/projects/terrorist-decision-making

LAURENCE ALISON, MICHAEL HUMANN AND SARA WARING

COMMUNICATING WITH CASUALTIES IN EMERGENCIES

Professor Laurence Alison and Drs Michael Humann and Sara Waring conducted CREST-funded research on live-exercise training events. You can read the full report as well as recommendations on how emergency responders can improve casualty communication on the CREST website at www.crestresearch.ac.uk/resources

When your life is at risk, your body goes into 'survival mode' to stay alive. Or does it? Both survivor testimonies and research reveal that there are many ways in which we can react.

One example of this comes from the fire at King's Cross Station in 1987, where some people bypassed safe exits in an effort to leave via the regular route that they always used but that led straight into the fire. This habitual behaviour, which may be attributed to humans being reticent to divert from regular routines, is thought to have contributed to the tragic death toll of 31. Another example is 'behavioural inaction', a form of cognitive paralysis in which people stop thinking for themselves and look to others for guidance on what to do. So, casualties show diverse behaviours: some self-mobilise, some freeze, some are hysterical and others do what they always do. For emergency services then, our proposal is to enable the self-mobilisers, direct the inert and calm the hysterical.

Thinking about how best to communicate with casualties requires understanding how people behave in emergencies, what they need to hear, and how they want to hear it. Answers to these questions can come from those who have experienced being casualties, but this comes with significant challenges. A useful alternative is to collect feedback from people who have played casualties in live exercises.

In recent research, funded by CREST, we collected data from 30 members of the public who played the role of casualties during a large-scale terrorism-related chemical weapons exercise, conducted on an underground railway network train and organised by UK emergency service practitioners. We found that, overall, volunteers playing the role of casualties during the exercise had a positive experience of their interaction with members of all three emergency services. This was reflected in their sense of trust and confidence in the individual agencies. Two key positive factors were (i) reassurance: the ability to reassure and calm the individual down and (ii) authoritative directness: the ability to give simple, clear and directive instructions.

However, casualties reported some significant delays in communication, with large periods of time where no further instruction was provided to them. Critically, they wanted to know what would happen next and (roughly) when. Even if explicit facts weren't known they wanted to be told that and given an indication of when they might get an update. For example, better to say, 'I'm David, I'm from fire and rescue. Some chemical has been set off in this carriage. We don't know what it is yet. Cover your face with this wet cloth. I need to get some equipment that will help me get you out. That won't happen within the next 10 minutes but we are working fast to get you out of here. You ARE going to be OK.' The alternative, of not giving these updates, results in casualties feeling anxious, uncertain and filling in their own gaps.

Most casualties expressed a willingness to be more active in the services response, including administering first aid. Identifying and facilitating the potential for self-mobilisation amongst casualties could help the relief effort, especially where it is impossible to provide direct assistance.

Our findings show that training first responders needs to go beyond the traditional hard skills around procedures and equipment deployment, to also provide communication and interpersonal skills as well as a basic understanding of the casualty 'mind set'.

To assist front-line responders in remembering key methods to communicate we recommend bearing in mind the following 'FEAR' mnemonic:

F – communicate clear FACTS about what has happened, when responders can get to casualties, what is going on, etc. And if you aren't clear make it clear you aren't clear!

E – establish a line of communication as EARLY as humanly possible.

A – where possible keep casualties ACTIVE in their own recovery and mobilisation. Research indicates a major factor in saving lives is the active participation of others in the incident in providing assistance.

R – updates and communication must be REGULAR. Even if there is nothing to update on just ensuring that casualties are told 'nothing has changed but we are still doing X Y and Z' creates an ongoing and important dialogue. Don't leave casualties for unspecified amounts of time and always indicate roughly when you will update them.

NEIL FERGUSON

UNDERSTANDING ENGAGEMENT IN VIOLENT EXTREMISM IN NORTHERN IRELAND

Professor Neil Ferguson draws on his work in Northern Ireland with former Loyalist and Republican combatants, to look at factors which occur regularly in accounts of engagement in violent extremism

Whenever we experience a terror attack, our initial response is to think how could someone do that? What would drive a person to kill others for political or ideological gain? Unfortunately the answers to these questions are not simple, and psychologists have struggled to derive adequate answers for decades.

The main problem lies with the dynamic and multifaceted range of factors involved in the transformation from civilian to violent extremist. Individual factors, community and societal context, and global ideological forces all have an influence. However, evidenced-based research is beginning to unearth some consistent findings and produce some useful insights.

The most common factor held prior to engagement in violent extremism is that of having a sense of being a member of a community which has been collectively victimised or unjustly treated. This condition is key to setting the contextual environment for radicalisation towards violent extremism to begin to be possible. This is clearly illustrated in the accounts of many of the former Republican paramilitaries I have interviewed. They spoke about how witnessing the brutality of the British Army or the Royal Ulster Constabulary (RUC) were key drivers for them to seek recruitment into the Irish Republican Army (IRA). These feelings of victimisation usually lead to a desire for revenge that drives initial engagement. Indeed, an individual's initial violence, while seemingly ideological or politically driven, may be no more than a reaction to events or perceived injustices experienced by the individual or their wider community.

It also important to note that the reaction to this injustice is not a simple Pavlovian stimulus. Rather, the incident can create a state of dissociation that forces an individual to consider their future, and make a conscious decision to pursue violence or join an armed group. Many of our interviewees who took action, reported periods of reflection after these victimising experiences during which they consciously considered how they would act to change the status quo, or hit back at those who were threatening their community. During this reflection they would weigh up their options within the context in which they were living. This act of reflection is an important consideration as many violent extremists project a view that they had no choice, claiming that the socio-political conditions forced them to use violence.

While a person may join a group whilst emotionally aroused in reaction to events around them, rather than through a radical ideological awakening, once they join a group then a number of psychological pressures push them into a deeper affiliation with the group and its ideological worldview. In Northern Ireland's segregated society Protestants and Catholics live separate lives. In what has been described as a 'benign form of apartheid', this segregation in homogenous groups has a significant impact on people's sense of identity, attitudes towards group members, perceptions of threat and biased attributions. However, once the individuals join extremist groups within these already segregated homogeneous partisan communities, the small group pressures are amplified. Inside these extremist cliques, the individuals are further insulated from the outside world and different opinions.

Being involved in these groups creates groupthink-like-conditions which foster conformity and remove barriers towards their involvement in extremist violence. Being active in these organisations also increases the sense of purpose, and feelings of empowerment, efficacy and decreased moral ambiguity. Being a member of a small secretive group also increases the sense of comradery and brotherhood, heightening the sense of collective identity. For most combatants I have interviewed, these aspects were further magnified during imprisonment. These experiences also provided the former combatants with a sense of purpose that sustained their activism beyond imprisonment and onto political or community work on their release.

These findings illustrate that any intervention to counter recruitment must focus on non-ideological factors and perceptions of injustice or grievances held by communities as this is the key precursor to involvement. These interventions must be able to respond to these perceptions without exacerbating them and further alienating the community. Once the individual is a member of an extremist group, the small group pressures and insulation from outside influences and discourses make it much more difficult to change the individual's course. Thankfully, Northern Ireland has also shown us that with changes in the political context, people of violence can become peacemakers, and that the activism that fuelled their violence can also fuel their peace-building work.

Neil Ferguson is Professor of Political Psychology at Liverpool Hope University. He leads a CREST-funded project on 'Learning and unlearning terrorism: The transition from civilian life into paramilitarism and back again during the conflict and peace process in Northern Ireland'. You can read about this research at www.crestresearch.ac.uk/projects

JAN-WILLEM BULLÉE

SOCIAL ENGINEERING: FROM THOUGHTS TO AWARENESS

Would you give your keys to a stranger? Probably not. However, Jan-Willem Bullée's research has shown that, in an office environment, 59% of participants did exactly that. He tells us why, here.

PSYCHOLOGICAL MANIPULATION

Most people underestimate the degree to which they will engage in insecure behaviour, something that criminals exploit through 'social engineering'. Our vulnerability to these kind of attacks is exploited by offenders who use psychological manipulation to make us assist them. These kind of attacks are successful since we use heuristics (i.e., rules of thumb) in our decision making. These mental shortcuts work well in most circumstances. However, when a heuristic fails, a cognitive bias occurs. A cognitive bias is mistaken thinking due to errors in reasoning or evaluation. There are several ways in which this tendency can be exploited to influence people to make it hard for them to say no. One tactic is reciprocity, whereby receiving a gift can make someone feel indebted and more likely to give something in return. A common example of this is when restaurants give customers a mint when presenting the bill, a gift which can result in bigger tips.

THREE ATTACKS

In my research, we performed three type of attacks in a controlled environment. During the first attack employees were called by an unknown and untrusted 'offender' who persuaded them to download and install some software. In this attack, the offender induced reciprocity by warning the victim about their PC being in danger. During the second attack, offenders visited employees in their offices and asked them to hand over their electronic office key. In the third attack, phishing emails were sent to office employees in an attempt to convince them to share network credentials.

NOBODY THINKS THEY WOULD FALL FOR THIS

As an outsider, it seems obvious that such social engineering schemes are scams. It is hard to believe that someone would fall for them. A survey among academic researchers in The Netherlands confirms this. In the survey, no-one reported that they would install the software from a cold call and only 3% reported that they would hand over their office key to a stranger. My experiments suggest otherwise. In total, 40% of the employees installed the software and 59% of the employees handed over their office key to a stranger.

TRAINING

On a positive note, there is hope. I divided those who participated in the first two attacks into groups. One group received information showing them how to recognise potential scams. This group performed better than a group which received no training, at both the installation of software (17% vs. 40%) and handing over office keys (37% vs. 59%). However, this improvement disappeared when the length of time between the information campaign and the attacks was increased.

LENGTH OF SERVICE MATTERS

My analysis of the subjects' socio-demographic characteristics in the three experiments showed that both target gender and age did not influence the outcome. However, in the email experiment, the victim's length of service with their employer did influence the outcome and had an interaction effect with age. This suggests that young employees with only a few years of service are those most vulnerable to phishing emails.

IMPLICATIONS FOR PRACTICE

I suggest that there are some important implications arising from these results.

1) Awareness-raising about social engineering reduces the probability of falling for a scam. Training should include how to recognise the tactics people use to influence victims and how to react.

2) Awareness-raising training is only effective for a short period of time. Therefore, a single round of training is insufficient. However, merely repeating the same message over and over again is also ineffective and could even be counterproductive. The solution is likely to lie somewhere in the middle; in regular repeat training with innovative approaches and materials.

3) People tend to be overly optimistic about their level of risk. My research discovered a difference between intended and actual behaviour. If people do not see the urgency of the problem, they may not accept any training or countermeasures. One explanation for this is the optimism bias (another cognitive bias), which can run along the lines of: 'I am less likely to be targeted by an offender. If I am targeted, I am better at resisting than someone else. Therefore, this training is not relevant to me.' Tackling and reducing this optimism bias should, therefore, be a part of awareness-raising training.

4) Vulnerable groups should get special attention. I found that young, recently hired personnel are most at risk. An easy way to reduce this vulnerability is to provide awareness training during induction. As I found no effect of gender or age I would suggest that there is no need for training targeted specially for men, women, younger or older colleagues.

Jan-Willem Bullée researches information security at the University of Twente.

MIRIAM S. D. OOSTINGA

COMMUNICATION ERROR HANDLING IN SUSPECT INTERVIEWS AND CRISIS NEGOTIATIONS

You arrive at a scene in which someone is standing on the ledge of a roof, threatening to jump down. You've been briefed and start a conversation with the hope of getting them down safely. But, in your haste, you use the wrong name. What do you say next? Should you say sorry, deny that you were wrong, or blame the person who briefed you?

This simple question was raised by a crisis negotiator in the UK. We went away to look up psychology and law research on the topic, but were surprised to discover that there was none. Even though errors are commonplace in conversations, and even more likely in high emotional and high-stake scenarios, nobody had examined them. My research is a response to this. It aims to better understand the effects of errors and how best to respond to them – an action referred to as communication error management. Together with colleagues I've assessed communication error management in both suspect interviews and crisis negotiations, and found some unexpected effects.

The first goal of our work was to understand the kinds of errors officers make in interaction, and how they try to respond. In interviews with professional crisis negotiators we found a clear distinction between three types of error: factual, judgment and contextual. An error of fact is a message that is objectively wrong, such as the use of the wrong name, date or place. An error of judgment is a message that is subjectively wrong, such as not adequately reflecting the thoughts and feelings of the other party. An error of context is a message that shows a failure to adhere to police practices or procedures.

We also found it possible to classify officers' responses into four categories: accept, apologise, attribute, and contradict. In an accept response, the error maker takes full responsibility. In an apologise response, the error maker takes responsibility and in a way, sympathises with the other party. In an attribute response, the error maker takes no responsibility and shifts the blame to a third party. In a contradict response, the error maker takes no responsibility and blames the conversation partner.

That's what people say they do. But how do errors make them feel? As you might expect, professional law enforcement officers find making errors distracting and stressful.

However, research in related domains has found that this negative impact can be reduced by taking an error management, rather than error prevention, approach. When taking an error management approach, errors are considered inevitable and are classified as opportunities from which one can learn. When taking an error prevention approach, errors are believed to be detrimental and should be prevented at all cost.

Is it rational to be concerned about errors? Probably. We have found that judgment errors negatively affect trust and rapport in suspect interviews. But, we did not find this negative effect in crisis negotiations. Surprisingly, in both type of interactions, there was a positive effect of errors, with suspects sharing more information after an error was made. Suspects share more, it turns out, in an effort to explain why the law enforcement officer was wrong.

The ultimate effect of an error is dependent on the response that is used after the error. An accept response is effective in re-establishing rapport and decreasing hostility. A contradict response threatens it. An accept response is more effective in suspect interviews. Apologies are more effective in crisis negotiations. A possible explanation for this latter difference is that the needs of the suspect may differ in these types of interactions. In a suspect interview, the suspect wants to make sure that the interviewer records the correct information, so a simple accept will do. In a crisis negotiation, the suspect needs attention and the sympathising tone of an apology addresses this need.

All in all, communication errors can be both positive and negative. From the eyes of law enforcement officers, errors increase distraction and stress, while errors of judgment predominantly have a damaging effect on the suspect. But ultimately the effect of an error is determined by how the maker of the error responds.

Miriam Oostinga is a PhD student in the Department of Psychology of Conflict, Risk and Safety at the University of Twente. Her research, with Professors Ellen Giebels and Paul Taylor, into communication error management is funded by the FBI's High-Value Detainee Interrogation Group. Want to read more about communication error management? Go to the author's publication list via the following link: https://miriamoostinga.com/publications

SAMANTHA MANN

HOW DOES A SMUGGLER BEHAVE?

A study on smuggling has disproved the myth that it is easy to spot smugglers by their evasive nonverbal behaviour. A disappointing finding? Not at all says Samantha Mann, who describes how her research can help make law enforcement strategies more effective, and also shape future efforts to find out what techniques may be useful.

Popular films and behind-the-scenes television shows would lead us to believe that smugglers leak signs of nervousness, in much the same way that those same sources portray the behaviour of liars in general. Smuggling, after all, is just a specific form of deception. Just as some liars may exhibit nervous behaviour, so may some smugglers. Of course, nervous smugglers are more likely to be apprehended by customs officers, reinforcing beliefs that this is how smugglers behave. But what about all the smugglers who succeed in their crime undetected?

DECEPTIVE BEHAVIOUR

Decades of research into deceptive behaviour has revealed that there is, in fact, no 'Pinocchio's nose.' No reliable, nonverbal behavioural cue indicative of deceit, however much we want there to be. Whilst subtle differences may be detected between groups of liars and truth tellers, these largely oppose the nervous behaviours popularly associated with lying and they tell us little about how to detect one liar at one point in time.

The problem is that there are several dimensions to what a liar may experience. These include anxiety about getting caught, which might lead to an increase in fidgety movements. But at the same time the liar may well experience an increase in cognitive load, and an urge to control behaviour, both of which result in a decrease in movement. Combine these experiences with other factors, such as what the lie is about, what the consequences of being caught are, and the liar's personality, experience, and relationship with the target, creates a myriad of moving parts that is hard to predict.

Professionals often argue that such findings are based on laboratory studies where the stakes are low for the liar, and do not resemble real-life, high-stake situations. It is true that the behaviour of the real-life, high-stakes liar, is hard to obtain in a form that may be examined. However, such studies do exist and corroborate the findings of laboratory studies. Hence, deception researchers have largely moved on from examining nonverbal behaviour in order to detect deceit. Instead they have turned their attention to verbal differences, or developing techniques, such as manipulating the interview, in order to distinguish liars from truth tellers.

The problem with detecting a smuggler is that there is only non-verbal behaviour to go on. This is true of any person with malicious intent among a crowd of people. Thus, as recent events have demonstrated, the problem of detecting the smuggler is an important one to solve.

THE BEHAVIOUR OF THE SMUGGLER: A RESEARCH STUDY

In a study conducted at the University of Portsmouth, fifty-two participants were invited to see if they could evade detection when smuggling an item on a short ferry ride over to the neighbouring town of Gosport (each taking part individually). They were told that there would be 'agents' on the boat looking out for suspicious passengers, and that they should try to avoid looking conspicuous and being detected. This was their only instruction. They could use any devices (e.g., mobile phone) that they wished to use, smoke, walk about or sit wherever they wished. They were to meet with a contact near the ferry terminal on the other side. The experimenter gave the participant a mobile phone to contact her in the event of any problem, which had the added advantage of being able to track the participant's precise location.

Two 'agents', posing as regular passengers and of whom one was disguised as a cyclist carrying a cycle helmet with a small GoPro camera attached, also travelled on the ferry to Gosport in order to covertly film each participant. Half of the participants smuggled the item on the way to Gosport whilst the other half went to Gosport without anything to smuggle, but received the item from the contact in order to smuggle it back. Hence half of the participants were covertly filmed when smuggling and half when they were not. All participants were interviewed at the end of their mission to discover what tactics they used to evade detection, and what thought processes they had. The videos, with participants' permission, were analysed for various behaviours, and then shown to another group of participants to see if they were able to detect who was smuggling and who was not.

Only eight of the participants realised that they were being filmed. How anxious participants felt about smuggling correlated with their anxiety levels measured in a personality questionnaire. Aside from this, there was nothing consistent about the tactics they employed, which varied wildly (for example, sitting amongst other people or sitting away from others, looking at everyone or avoiding all eye contact). Similarly, analysis of the video footage revealed no consistent behavioural cues. This finding was corroborated by the fact that participants in a further study were only 48% accurate at detecting who was smuggling and who was not.

THE NEXT STEP IN DETECTING SMUGGLERS

As anticipated, participants varied wildly in their behaviour and tactics when smuggling. Whilst it is true that the participants in this study were probably not practiced in the art of smuggling, based on deception research, we assume that this reflects real life where some may exhibit detectable nervous behaviour and many will not. Hence the most effective solution, as in other realms of deception research, is to devise an easily implementable technique to distinguish between smugglers and innocents. For example, by having 'agents' approach and stand uncomfortably close to the participant and appear to detect them, but without saying as much, to see if doing so prompts a different reaction in smugglers to those who are not smuggling. This is what we are currently investigating.

Dr Samantha Mann is a Senior Research Fellow at the University of Portsmouth.
This study was funded by CREST.

A TO Z OF DECISION MAKING

ANCHORING is the irrational tendency for people to root their judgements during decision making to the first piece of information they receive, even if this information is arbitrary or misleading.

BIASES – as in cognitive biases – are the resulting errors in decision making that arise from heuristic 'rule-of-thumb' processing. They occur when individuals disengage with rational cognitive processing and instead rely on intuitive (albeit faulty) mental shortcuts.

CONSEQUENCE CHOOSING is a process involved during more deliberative decision-making tasks, wherein decision makers consider the longer-term outcomes of their potential choices, rather than focusing on immediate- or short-term preferences.

DEVIL'S ADVOCATE TECHNIQUE involves purposely assigning a team member to argue against the position of the majority. It is thought to reduce groupthink.

ECOLOGICAL INFERENCE PROBLEM is the technical name given to the fact that one can't successfully make inferences about an individual based on data captured at the aggregate level.

FORESTALLING is a decision strategy that can be used to buy time when coping with uncertainty. It involves preparing various courses of action to counter potential negative outcomes for choices, and is often accompanied with deferral and choice delay.

GOALS act as motivational markers that orient decision making and direct human behaviour around purposeful outcomes.

HEURISTICS are the mental shortcuts or 'rules-of-thumb' that people use when making judgements. Although heuristics can be constructive, they can also lead to faulty or biased decision making.

INERTIA – as in decision inertia – is the maladaptive process of redundant deliberation over a choice for no meaningful gain. It has been observed in high-stakes decision-making contexts, wherein the decision maker cannot disengage with cognitive processing (i.e., due to organisational responsibilities), but feels unable to commit to a choice.

JUDGEMENT AND DECISION-MAKING (JDM) is a multi-disciplinary approach to decision-making research based on experimental studies that seek to predict or explain judgements and decisions using quantified or mathematical models.

KAHNEMAN (Daniel) is the Nobel prize-winning psychologist for his research on economic decision making. He is most famous for his work, with Amos Tversky, on Prospect Theory, heuristics and biases.

LOSS AVERSION refers to a bias in human decision making wherein individuals will take far higher risks to avoid losses than they would to acquire equivalent gains. If given the choice to take a sure £100 or gamble to win £200 (or nothing), most people will take the £100; but when asked to lose a certain £100 or gamble to lose £200 or nothing, most people will take the gamble. People take higher risks to avoid loss.

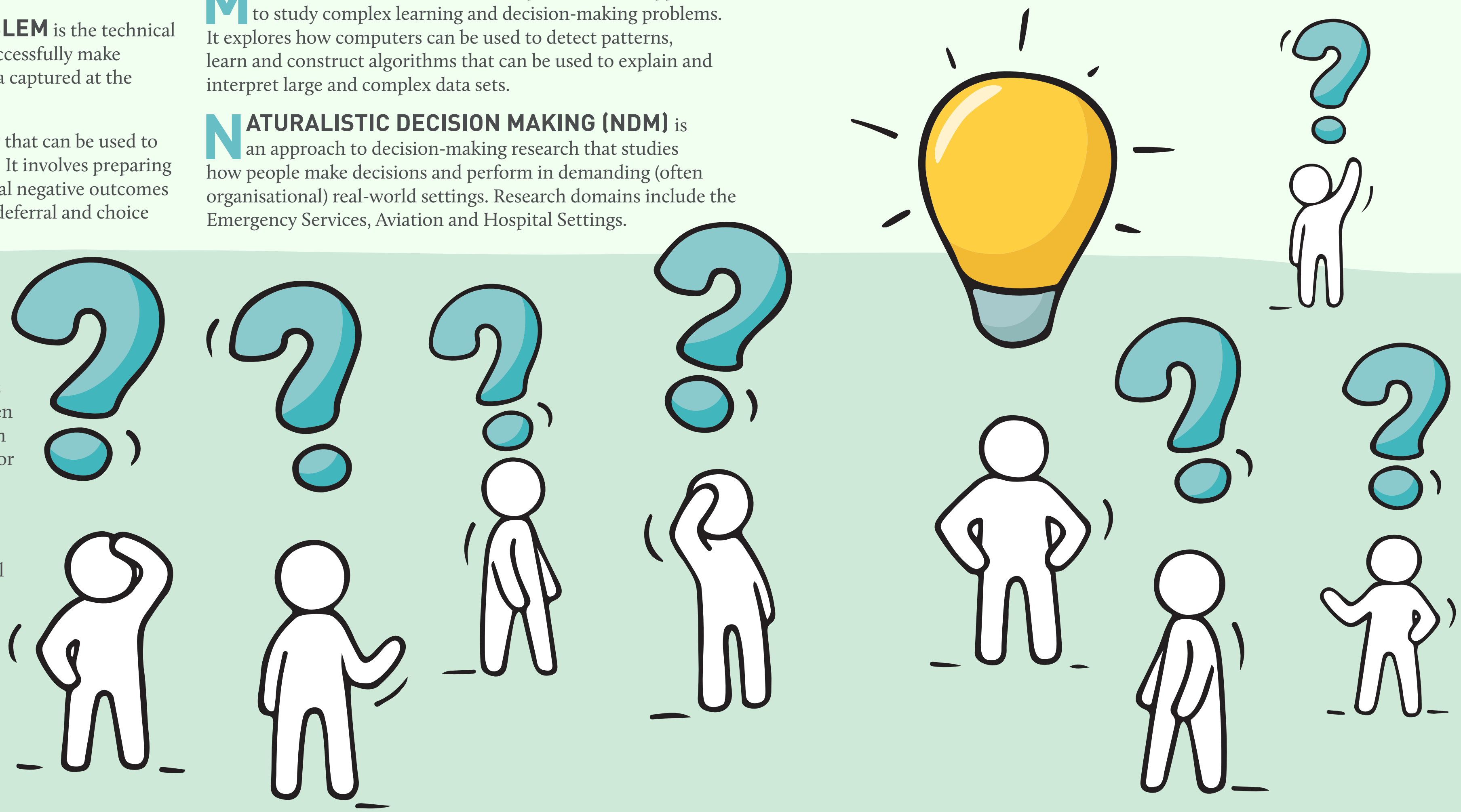
MACHINE LEARNING is a computer sciences approach to study complex learning and decision-making problems. It explores how computers can be used to detect patterns, learn and construct algorithms that can be used to explain and interpret large and complex data sets.

NATURALISTIC DECISION MAKING (NDM) is an approach to decision-making research that studies how people make decisions and perform in demanding (often organisational) real-world settings. Research domains include the Emergency Services, Aviation and Hospital Settings.

ORGANISATIONAL DECISION-MAKING research explores how people make decisions in work domains. This kind of research seeks to identify how organisational decision making can be supported (e.g., decision support tools) and further seeks to unpack expertise in work domains to accelerate its development with novice or new trainees.

PROSPECT THEORY is a descriptive model used to explain how people make decisions under conditions of uncertainty and risk. It posits that individuals make decisions based upon probabilistic estimates linked to losses and gains, but these estimates can be subjectively skewed due to cognitive heuristics and biases (e.g., Loss Aversion).

QUANTIFYING OUTCOMES objectively is the holy grail of decision making according to Expected Utility Theory. But we know from psychology that the capacity for objective quantification is rare due to cognitive and environmental constraints that bound rationality.



REPRESENTATIVENESS is a heuristic that describes how people assume prototypical knowledge about something based on past experience with something similar (e.g., stereotyping).

SYSTEM 1 OR SYSTEM 2 THINKING – Kahneman's dichotomy on how humans make decisions: using fast and frugal intuitive system one thinking; or slower and effortful system two thinking.

THIRTY-SEVEN PERCENT is the optimal amount of your committed time that you should spend exploring options – looking – before you commit – leaping – to buying a house, to dating a partner, etc. Google the 'Secretary problem'.

UNCERTAINTY is a sense of doubt that blocks or delays decision making and action. It is linked to perceived risk about a decision problem and judgements on current and anticipated future states. People try and cope with uncertainty by adapting their cognitive processing styles (e.g., relying on heuristics; using decision support systems).

VARIABILITY in decision making is inherent in the real world. People can vary the way they approach the same decision problem due to numerous factors including, expertise in the decision domain, personality and cognitive processing styles.

WAR GAMES are military exercises used to test warfare strategies and identify combat readiness. Interestingly, playing war games has been found to lead to overconfidence in expectations of success, with this effect especially pronounced in men.

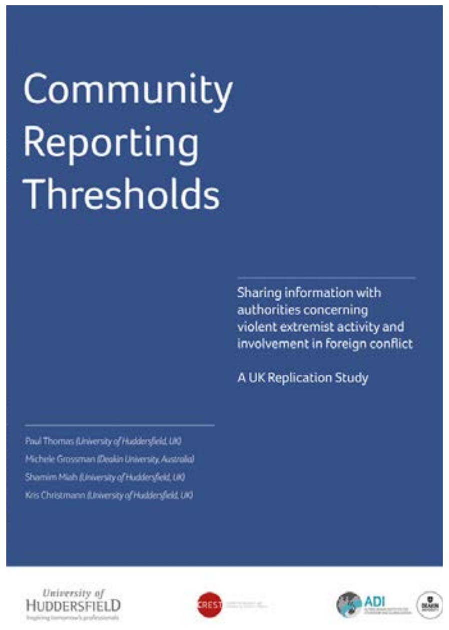
XTREME ENVIRONMENTS are high-risk and highly uncertain contexts that place huge demands on the physical, psychological and interpersonal skills of decision makers. They are of particular interest to scholars engaged in NDM research; for example, decision making in military contexts.

YES vs NO or, as they are defined in the literature, promotion focused vs. preventative focused. The former looks outward toward new horizons. The latter makes sure everything is completed and correct with the status quo before moving on. Both are critical to successful teams.

ZERO-SUM GAMES are used to explore conflict and cooperation between decision makers, wherein one player's gains are equivocal to the losses of another player so that the sum of outcomes is always zero (e.g., Poker - where the amounts won by some players are equal to the combined losses of other players).

MORE ON DECISION MAKING...

Want to read more about decision making in different contexts? Visit www.crestresearch.ac.uk/tag/decision-making for an up-to-date list of resources on decision making, funded by the Centre for Research and Evidence on Security Threats.



Community Reporting Thresholds

Sharing information with authorities concerning violent extremist activity and involvement in foreign conflict

A UK Replication Study

Paul Thomas (University of Huddersfield, UK)
Michele Grossman (Deakin University, Australia)
Shamim Miah (University of Huddersfield, UK)
Kris Christmann (University of Huddersfield, UK)

COMMUNITY REPORTING THRESHOLDS

What are the barriers to reporting on a friend or family member who are suspected of involvement in violent extremism? Led by Professor Paul Thomas from the University of Huddersfield (UK) and Professor Michele Grossman from Deakin University (Australia), this project, which built on an earlier Australian study, developed a new, localised and contextually-sensitive understanding and approach to community reporting issues in the UK.

This report, and accompanying executive summary, focuses on identifying triggers, thresholds and barriers which may stop someone from reporting. It includes the key findings and conclusions of the research, for both community respondents and professional practitioners.

You can download these reports for free, from www.crestresearch.ac.uk/resources

CREST has also funded projects on terrorist decision making and decision making in critical incidents.

Visit www.crestresearch.ac.uk/project to find out more.

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

NICOLA POWER – DECISION-MAKING DURING EMERGENCIES (PAGE 8)

- Claudia van den Heuvel, Laurence Alison, Jonathan Crego. 2012. How uncertainty and accountability can derail strategic 'save life' decisions in counter-terrorism simulations: A descriptive model of choice deferral and omission bias. *Journal of Behavioral Decision Making*, 25(2), 165-187. Available at: https://goo.gl/Ejs4ig
- Laurence Alison, Nicola Power, Claudia van den Heuvel, Sara Waring. 2015. A taxonomy of endogenous and exogenous uncertainty in high-risk, high-impact contexts. *Journal of Applied Psychology*, 100(4), 1309-1318. Available at: https://goo.gl/AqG1C5
- Claudia van den Heuvel, Laurence Alison, Nicola Power. 2014. Coping with uncertainty: police strategies for resilient decision-making and action implementation. *Cognition, Technology & Work*, 16(1), 25-45. Available at: https://goo.gl/BQ9HxL
- Laurence Alison, Nicola Power, Claudia van den Heuvel, Michael Humann, Marek Palasinksi, & Jonathan Crego. 2015. Decision inertia: Deciding between least worst outcomes in emergency responses to disasters. *Journal of Occupational and Organizational Psychology*, 88(2), 295-321. Available at: https://goo.gl/De6Vva
- Sabrina R. Cohen-Hatton, Philip Butler, Robert Honey. 2015. An investigation of operational decision making in situ: Incident command in the UK Fire and Rescue Service. *Human Factors*, 57(5), 793-804.
  Available at: 🔓 https://goo.gl/GhP9yi
- Sabrina R. Cohen-Hatton, Robert Honey. 2015. Goal-oriented training affects decision-making processes in virtual and simulated fire and rescue environments. *Journal of Experimental Psychology: Applied*, 21(4), 395-406. Available at: 🔓 https://goo.gl/musZtx

RENATE GEURTS – WHY PROFESSIONALS ARE NEEDED TO ASSESS THREATS OF VIOLENCE (PAGE 10)

- Renate Geurts, Pär Anders Granhag, Karl Ask, Aldert Vrij. 2017. Assessing threats of violence: Professional skill or common sense? *Journal of Investigative Psychology and Offender Profiling*. Available at: https://goo.gl/exkhjb
- Paul Slovic, Melissa L. Finucane, Ellen Peters, Donald G. MacGregor. 2004. Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk Analysis*, 24, 311-322. Available at: 🔓 https://goo.gl/4x5Na4
- Itiel E. Dror. 2016. A hierarchy of Expert Performance. *Journal of Applied Research in Memory and Cognition*, 5, 121-127. Available at: https://goo.gl/Twt8vz
- Arthur S. Elstein, Alan Schwarz. 2002. Clinical problem solving and diagnostic decision making: Selective review of the cognitive literature. *British Medical Journal*, 324, 729-732. Available at: https://goo.gl/s9JMZG
- Laurence Alison, Emma Barrett, & Jonathan Crego, J. (2007). Criminal investigative decision making: Context and process. In R. R., Hoffman (Ed.), *Expertise out of context: Proceedings of the sixth international conference on naturalistic decision making* (pp. 79-95). London & New York: Taylor & Francis Group.
- Laura S. Guy. 2008. *Performance indicators of the structured professional judgment approach for assessing risk for violence to others: A meta-analytic survey*. Doctoral dissertation, Simon Fraser University. Available at: 🔓 http://summit.sfu.ca/item/9247
- Kevin S. Douglas, James R. P. Ogloff, Stephen D. Hart. 2003. Evaluation of a model of violence risk assessment among forensic psychiatric patients. *Psychiatric Services*, 54, 1372-1379. Available at: 🔓 https://goo.gl/xM117v

SIMON RUDA – MEASURING DECISION MAKING (PAGE 12)

- Michael Hallsworth, John A. List, Robert D. Metcalfe and Ivo Vlaev. 2017. The behavioralist as tax collector: Using natural field experiments to enhance tax compliance. *Journal of Public Economics*, 148, pp.14-31. Available at: 🔓 http://www.nber.org/papers/w20007
- The Behavioural Insights Team. 2017. *Update Report 2015-16*. Available at: 🔓 https://goo.gl/HJnEQC
- Leslie K. John, Alessandro Acquisti, George Lowenstein. 2011. Strangers on a Plane. *Journal of Consumer Research*, 37. Available at: 🔓 https://goo.gl/Dtq3g5
- Lorraine Mazerolle, Sarah Bennett, Emma Antrobus, Elizabeth Eggins. 2012. Procedural justice, routine encounters and citizen perceptions of police: Main findings from the Queensland Community Engagement Trial (QCET). *Journal of Experimental Criminology*, 8(4), 343–367. Available at: https://goo.gl/vrALqr

JULIE GORE, PAUL WARD, GARETH CONWAY – NATURALISTIC DECISION MAKING AND UNCERTAINTY (PAGE 14)

- Gary Klein. 2016. The-naturalistic-decision-making-approach. *Psychology Today*. Available at: 🔓 https://goo.gl/QeCT3D
- Julie Gore, Gareth E. Conway. 2016. Modeling and Aiding Intuition in Organizational Decision Making: A Call for Bridging Academia and Practice. *Journal of Applied Research in Memory and Cognition*, 5(3): 331-334. Available at: http://www.sciencedirect.com/science/article/pii/S2211368116301498
- Julie Gore and Paul Ward (eds). 2017. *Naturalistic Decision Making and Uncertainty – Proceedings of the 13th bi-annual international conference on Naturalistic Decision Making*. Available at: 🔓 https://goo.gl/kStpe2
- Julie Gore and Claire McAndrew. 2009. Accessing Expert Cognition. *The Psychologist* Vol 22: 218-219. Available at: 🔓 https://thepsychologist.bps.org.uk/volume-22/edition-3/methods-accessing-expert-cognition

JAN-WILLEM BULLEE – SOCIAL ENGINEERING: FROM THOUGHTS TO AWARENESS (PAGE 22)

- Jan-Willem H. Bullée, Lorena Montoya, Marianne Junger, and Pieter H. Hartel. 2016. Telephone-based social engineering attacks: An experiment testing the success and time decay of an intervention. In A. Mathur and A. Roychoudhury, (Eds.), *Proceedings of the inaugural Singapore Cyber Security R&D Conference (SG-CRC 2016)*, Singapore, Singapore, volume 14 of Cryptology and Information Security Series, pages 107–114, Amsterdam: IOS Press. Chapter available at: 🔓 https://research.utwente.nl/en/publications/telephone-based-social-engineering-attacks-an-experiment-testing-
- Jan-Willem H. Bullée, Lorena Montoya, Wolter Pieters, Marianne Junger, and Pieter H. Hartel. 2015. The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Journal of Experimental Criminology*, 11(1):97–115. Available at: https://link.springer.com/article/10.1007/s11292-014-9222-7
- Jan-Willem H. Bullée, Lorena Montoya, Marianne Junger, and Pieter H. Hartel. 2017. Spear phishing in organisations explained. *Information and Computer Security*. Available at: http://www.emeraldinsight.com/doi/pdfplus/10.1108/ICS-03-2017-0009

MIRIAM S. D. OOSTINGA – COMMUNICATION ERROR HANDLING IN SUSPECT INTERVIEWS AND CRISIS NEGOTIATIONS (PAGE 24)

- Miriam S. D. Oostinga, Ellen Giebels, Paul J. Taylor. 2017. 'An error is feedback': The experience of communication error management in crisis negotiations. *Police Practice and Research*. Advance online publication. Available at: 🔓 http://www.tandfonline.com/doi/full/10.1080/15614263.2017.1326007
- Nicoletta G. Dimitrova, Edwin A. J. van Hooft, Cathy van Dyck, Peter Groenewegen. 2016. Behind the wheel: What drives the effects of error handling? *The Journal of Social Psychology*. Available at: https://goo.gl/vYm5nD

SAMANTHA MANN – HOW DOES A SMUGGLER BEHAVE? (PAGE 26)

- Samantha Mann, Aldert Vrij, Ray Bull. 2002. Suspects, lies, and videotape: An analysis of authentic high-stake liars, *Law and Human Behavior*, 26, 365-376. Available at: https://goo.gl/tGWKwL
- Aldert Vrij. 2008. Detecting *Lies and Deceit: Pitfalls and Opportunities*. (2nd Ed.) Chichester: John Wiley & Sons.

CREST

CENTRE FOR RESEARCH AND
EVIDENCE ON SECURITY THREATS

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

THE CENTRE FOR RESEARCH AND EVIDENCE ON SECURITY THREATS

CSR is produced by the Centre for Research and Evidence on Security Threats (CREST). CREST is funded by the UK's security and intelligence agencies to identify and produce social science that enhances their understanding of security threats and capacity to counter them. CREST also receives funding from its six founding partners (the universities of Bath, Birmingham, Cranfield, Lancaster, Portsmouth and West of England). Its funding is administered by the Economic and Social Research Council (ESRC Award ES/N009614/1), one of seven UK Research Councils, which direct taxpayers' money towards academic research and training. The ESRC ensures the academic independence and rigour of CREST's work.

CREST has established a growing international network of over 100 researchers, commissioned research in priority areas, and begun to tackle some of the field's most pressing questions.

'There really is some impressive work going on. Yet, all that effort is irrelevant if practitioners, policy-makers, and other stakeholders do not get to hear about it. *CREST Security Review* is one way we will keep stakeholders informed not only on what CREST is doing, but also on the best research from around the world.'
Professor Paul Taylor, CREST Director

For more information on CREST and its work visit
www.crestresearch.ac.uk and find us on Twitter, Facebook and LinkedIn.

Lancaster University

UNIVERSITY OF BIRMINGHAM

University of Portsmouth

UNIVERSITY OF BATH

Cranfield University

UWE BRISTOL University of the West of England

E·S·R·C ECONOMIC & SOCIAL RESEARCH COUNCIL