AUTUMN 2016 / ISSUE 02

CREST SECURITY REVIEW

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

CREST

Cyber Security

Contents

CREST SECURITY REVIEW

Editor – Matthew Francis
Guest Editor – Debi Ashenden
Illustrator – Becky Stevens
Designer – Emma Smart, wash-design.co.uk

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

Highlights

BUILDING GOOD RAPPORT IN INTERVIEWS

Interviews are most effective when there is good rapport with suspects. Laurence Alison, Michael Humann and Sara Waring analysed 1,000 hours interviews to find out what works – p6

THE CONTINUING GROWTH OF RELIGIOUS EXTREMISM, AND HOW TO COUNTER IT

The extremist drift is not just Islamic – Linda Woodhead looks at what the future holds for religious belief – p26

From the Editor

This issue of *CSR* considers social science contributions to cyber security. Cyber security is important to us all. Whether it's our phone's contact list or our account with the electricity provider, services that we rely on hold our personal information in databases connected to the internet and potentially vulnerable to attack.

Recognising this, the UK Government has released a new National Cyber Security Strategy. They pledge to invest £1.9 billion over the next five years to make the UK secure and resilient to cyber threats. However, they also acknowledge that cyber security requires new thinking and that 'maintaining the current approach is insufficient.' Where is this new thinking going to come from? Physical and personnel security are intertwined with cyber security and the national strategy reflects this: 'cyber security is not just about technology. Almost all successful cyber attacks have a contributing human factor.' The new strategy recognises the need for organisations to develop a strong personnel security culture and it is the social and behavioural sciences that will find effective ways to deliver this.

The motivations of those carrying out cyber attacks aren't necessarily different from those of the caricatured stripy-shirted burglar creeping into your home – Marcus Rogers discusses the hacker mind set on page 18. In fact, often the crimes themselves are nothing new. They've just been made easier or have more impact because the internet affords criminals more reach and anonymity. Pete Burnap and Matt Williams consider this issue and the differences between crimes that are enabled by information and communications technology, and those that are dependent upon it (page 16).

As this issue's *Guest Editor*, Debi Ashenden reminds us on page 10 that breaches of security aren't just the fault of criminals. Sometimes the responsibility rests with employees who think they are acting in their employer's best interests. These 'everyday insider threats' are critical to understand how organisations can make significant improvements to their cyber security.

The importance of thinking about humans when improving data service security is considered by René Rydhof Hansen and Lizzie Coles-Kemp on page 12. They argue for a creative approach to how we think about and design security, which includes considering users' needs and experiences.

Elsewhere in this month's *CSR* we review research that underpins evidence-based practice, reporting on the High Value Detainee Interrogation Group research programme and the new PETRAS Internet of Things research hub. Elizabeth Morrow writes on the EDL's loyal foot-soldiers and we have a long-read from Linda Woodhead on the future of religious belief and how the policies of governments and national churches might inadvertently lead to more, rather than less, extremism. This article foreshadows our next issue of *CSR*, which considers the transmission of ideas and beliefs.

If you'd like to know more about any of the research featured in *CSR*, or you have other comments, contact me at **m.d.francis@lancaster.ac.uk**

Terrorists' use of messaging applications

Matthew Francis and Emma Barrett look at how emerging technologies have changed terrorist behaviour in the past and suggest that we should think about the implications of innovations in messaging applications.

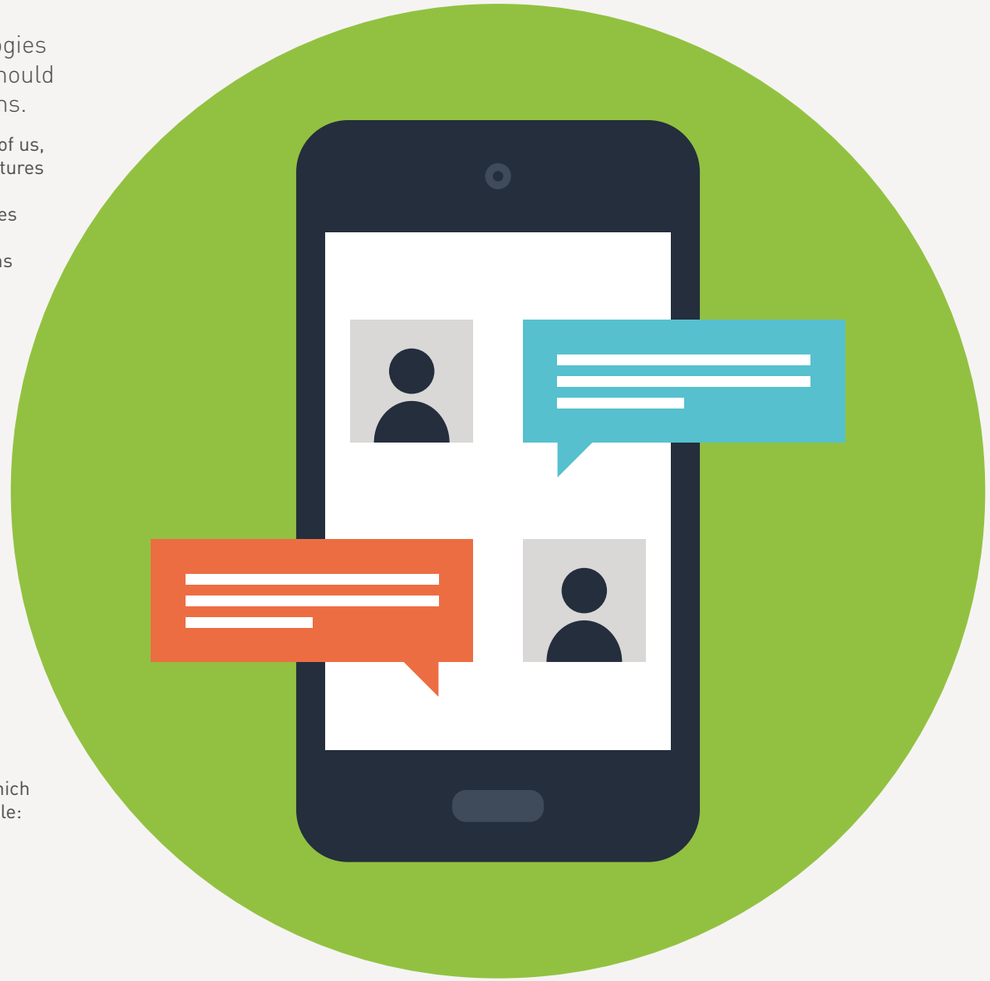
Terrorists and criminals, like the rest of us, need to communicate and, like the rest of us, they look out for ways of communicating that meet their particular needs. Some features of messaging applications may make them more attractive than others to terrorists when co-ordinating and planning their activities or distributing propaganda – features like encryption and anonymity, for example. As the current debate on encryption acknowledges, the use of apps for illicit communications has important ramifications for counter-terrorism, and not just in providing new ways to carry on old crimes.

People exploit emerging technologies for criminal or terrorist ends, but emerging technologies may also have qualities that enable or facilitate new types of criminal behaviour. There's nothing new about this. Consider the early adoption of the printing press by Pietro Aretino (1492-1556) to disseminate illicit pornographic material, and the way in which more recently the development of search engines aids the collection of illegal images of children.

In 1878, Russian revolutionary Vera Zasulich committed what has been described as the first act of non-state terrorism: the assassination of a city governor. This act of political violence was possible because of the development of the powerful British Bulldog revolver, which was compact enough to be hidden under her shawl. Until then her only choices had been bulky Smith & Wesson revolvers, meaning that her plans to carry out a political assassination had remained on the drawing board.

As these examples demonstrate, both how technology can be used for current purposes and what new uses it might facilitate are issues that need thinking through. So in the case of messaging applications what are some of their characteristics that might be attractive to criminals and terrorists, and what new forms of terrorist activity might they enable?

A guide produced by CREST assesses some of the key features, and applications, which are attractive to illicit use. Three categories of characteristics are particularly notable:



PRESENCE

This relates to the kind of information which tells users when someone was last online, their location and whether they have read messages. For example, with Telegram, users can control the timestamps of their messages, disabling them or replacing them with approximate times.

VERIFICATION

Using an email address or mobile number to validate identities are examples of the kind of processes that may, or may not be strictly enforced by some applications. Whether identities are verified or not can influence whether people trust those they communicate with. Twitter is a high-profile example of a networking service which supports messaging but which doesn't require verification.

ANONYMITY

Users may be able to conceal their identities by using pseudonyms or create accounts under different names that are not linked to their real contact details. The messaging application FireChat is one example of apps which allow messages to be sent from usernames as opposed to mobile numbers. FireChat users are not required to use real names so can send messages anonymously.

NOVEL FEATURES

Telegram's self-destructing messages and FireChat's Bluetooth connectivity (which circumvents telecom networks altogether) are of course intended by the manufacturers for benign use, although we need to consider how they might be used for malign purposes too. To be successful, terrorists and criminals need to keep their illicit activities secret, so it's no surprise that they are drawn to communication methods that offer the potential for encryption and anonymity.

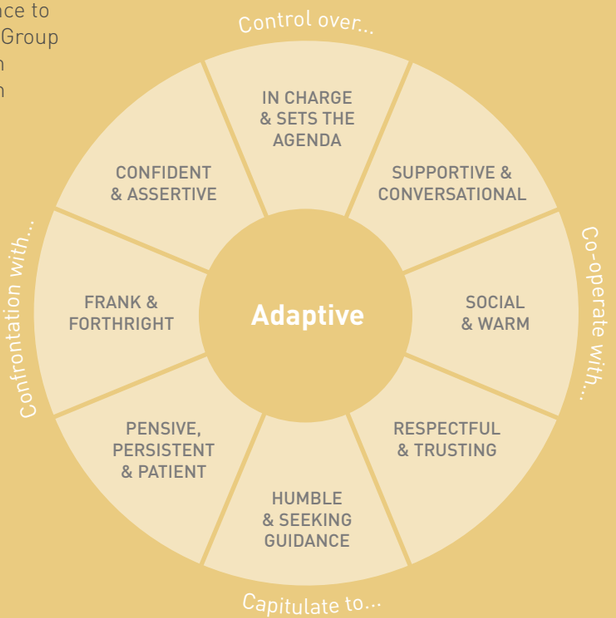
But as well as thinking about how criminals and terrorists use such apps to carry out their 'usual' activities, we should also be aware of the new activities that innovation in messaging apps could trigger. Researchers have pointed out that terrorists' ability not just to reach out to a wide audience online but to engage that audience in two-way conversation has enabled the development of a virtual community – something that is difficult to achieve with traditional broadcast media. New messaging applications allow that communication to become ever more personalised and ever less detectable. Without the assurance of anonymity, the plans of someone interested in engaging with that virtual community might – like Zasulich's early assassination plans – remain on the drawing board. Encrypted apps thus reduce one barrier to engagement.

The CREST Introductory Guide: Messaging Applications, *is available to download for free at www.crestresearch.ac.uk/resources.*
This article originally appeared on the CREST website. You can read it and the research it is based on at https://crestresearch.ac.uk/comment/terrorists-use-of-messaging-applications/.

LAURENCE ALISON, MICHAEL HUMANN AND SARA WARING

BUILDING GOOD RAPPORT IN INTERVIEWS

Most of us find it easier to talk to and cooperate with people with whom we have good rapport. It's no surprise that the same is true in police interviews with terrorism suspects. There is good evidence to support this too. The High-Value Detainee Interrogation Group (see page 22) funded CREST researcher Laurence Alison and his team to study the components of good rapport in interviews with terrorist suspects. Here they introduce the Observing Rapport-Based Interpersonal Techniques (ORBIT) tool, developed through that research, and explain how it is now informing the training and assessment of interviewers in the field.



The Observing Rapport-Based Interpersonal Techniques (ORBIT) tool was developed by our research team at the University of Liverpool, based on analysis of more than 1,000 hours of video footage of interviews with some of the most difficult terrorist suspects. Ours is the only field-based operational study of such interviews to date. It provides a contemporary evidence base of 'what works' in reducing counter-interrogation strategies and resistance and maximising intelligence, information and evidence gain.

We drew on Motivational Interviewing (MI) research to guide our research on interviewing. MI was originally developed in the therapeutic community, but it is now widely used to address problems in health care and psychological services. It is used as a way of strengthening an individual's motivation for change, based on a facilitative approach to communication. An MI approach aims to draw out the thoughts of the interviewee whilst not placing any demands on the interviewee to cooperate. It is based on five principles:

Autonomy
Providing choice for the interviewee.

Acceptance
Accepting the views, beliefs and explanations given by an interviewee without judgement.

Adaptation
To adapt to changes or developments in the interviewee's account throughout the interview.

Evocation
To draw out the interviewee's thoughts, beliefs or feelings without putting forward your own views.

Empathy
To show consideration for the immediate or longer-term concerns of the interviewee, to understand the perspective of the interviewee without accepting or respecting their views, and to seek clarification and understanding.

We hypothesised that effective suspect interviews would also be based on these five principles, and in particular that effective interviewers would build rapport by adopting different skills and techniques in response to the way in which the suspect is interacting with them. There is a full spectrum of positive and negative modes of relating, and we looked at whether or not effective interviewers used all modes in a versatile and competent way. For example, were they able to challenge and be authoritative but do so within a broader empathic and accepting context? We expected that effective use would increase the amount of useful information elicited from the suspect.

The next step was to determine how these principles could be observed from the behaviours of interviewers and interviewees. In our ORBIT model, we mapped the possible types of interviewer-interviewee interactions against two 'interpersonal circles' (see left and below). One circle shows adaptive responses (i.e. responses that lead to a better interview outcome) and the other shows maladaptive responses (i.e. those leading to a poor outcome). Each circle has two dimensions: a 'Cooperation – Confrontation' axis and a 'Capitulation – Control' axis:

Control
The way in which the interviewer directs the interview.

Capitulate
The approach taken to give up resistance towards a suspect.

Confront
The approach taken to oppose or challenge a suspect.

Co-Operate
The approach taken to work together to reach a goal.

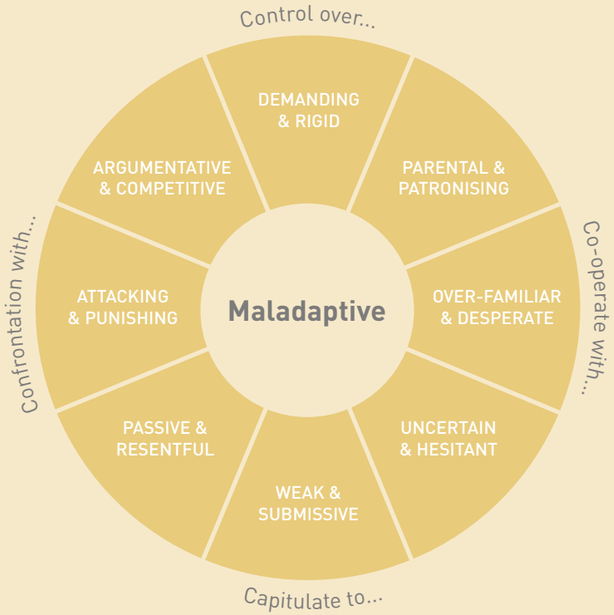
Based on frameworks developed in collaboration with expert interviewers across the police and security services, we analysed audio and video recordings of interviews with 29 convicted terrorist suspects across multiple interviews. We coded behaviours using the Interpersonal Behaviour Circles and analysed the amount of useful intelligence and evidence generated in the interviews. We also identified positive (and negative) styles of interpersonal relating including:

Sensitivity
Responsiveness (or lack thereof) to the suspect's interpersonal state.

Competence
Absence (or presence) of maladaptive interpersonal behaviours

Versatility
Use of a diverse (or limited) range of interpersonal behaviours.

Our analyses showed that interviewers were most effective when they were interpersonally sensitive (able to accurately respond to the interpersonal cues from the interviewee), competent (able to adopt only adaptive interpersonal behaviours and resist using any maladaptive ones) and versatile (able to display a broad range of interpersonal behaviours). In contrast, an inability to be responsive to the interviewee's particular relating style (insensitivity), the adoption of maladaptive interpersonal behaviour (incompetence), and the inability to utilise a range of interpersonal behaviours (rigidity) increased resistance and shut down further interactions.



Alongside this general pattern, three key findings stood out:

- Both interviewers and interviewees expressed predominantly adaptive behaviours.
- Adaptive interviewer behaviours produced adaptive interviewee behaviours - which in turn increased cooperation and the information received.
- Maladaptive interviewer behaviour produced maladaptive detainee behaviour - which decreased cooperation and information gain.

We are feeding our evidence back into training programmes, including the national advanced counter terrorism interviewing course as well as more specialised interview training (including child protection). They are helping interviewers to increase the effectiveness of interviewing through maximising the amount of information received whilst minimising resistance to cooperating.

Our research is now focused on how skills are used at different points in interviews as well as understanding specific details on areas where interviewers make a breakthrough in their interactions, or come up against significant hurdles. By developing our understanding of these critical moments, we can begin to help interviewers recognise and make the most of them.

Professor Laurence Alison, Dr Michael Humann and Dr Sara Waring are undertaking research for CREST on decision-making in the emergency services during critical incidents. You can read more about this project on the CREST website at www.crestresearch.ac.uk.

JEREMY WATSON, UNIVERSITY COLLEGE LONDON
EMIL LUPU, IMPERIAL COLLEGE

PETRAS – CYBER SECURITY OF THE INTERNET OF THINGS

A research hub to fill knowledge gaps and promote safe and secure use of the Internet of Things

TRANSPORT & MOBILITY | HEALTH & CARE | DESIGN & BEHAVIOUR

At the beginning of 2016, the PETRAS Hub consortium of nine leading UK universities was awarded £9.8m by the Engineering and Physical Science Research Council (EPSRC). PETRAS brings the universities together with around 50 user partners representing both the private and public sectors.

STRATEGIC REVIEW OF IOT

Following a strategic review by the UK Government, *'The Internet of Things: making the most of the Second Digital Revolution'* was published in 2014. It emphasised the economic importance of the Internet of Things (IoT), which would only be realised by ensuring its cyber security and trustworthiness while not standing in the way of vibrant technical and business development. The government response was to create the £40m IoTUK initiative, which funds the PETRAS hub amongst other initiatives.

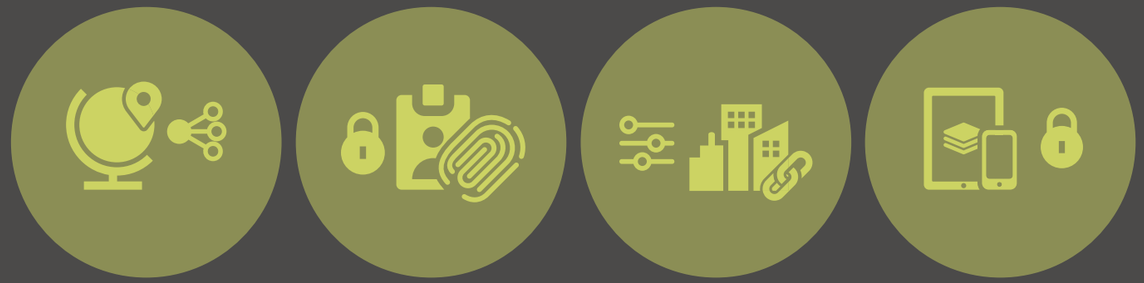
PRINCIPLES OF THE PETRAS HUB

The review highlighted a knowledge and capability gap in the ability to look at IoT (or indeed other) cyber security from an integrated socio-technical viewpoint. Collaborative thinking across social and physical science disciplines was needed from project identification to execution. This principle has guided the vision for PETRAS.

PETRAS stands for Privacy, Ethics, Trust, Reliability, Acceptability and Security – headings that have relevance to both technical and social science. They are all important in ensuring the successful adoption of the Internet of Things. The PETRAS hub is founded on these six themes, and emphasises in equal measure, the physical and social science aspects of the adoption of new IoT technology. The academic partners are made up of a cross-disciplinary Hub team of UCL, Imperial College, Oxford, Leicester and Warwick, augmented by four Spoke contributors at Surrey, Southampton, Cardiff and Edinburgh, who provide specialist contributions. Additionally, PETRAS boasts a large cohort of user and research partners in the private sector (ranging across banking, through healthcare to mobile telecommunications), the public and NGO sectors. 'Impact Champions' working in the PETRAS management team ensure good bidirectional connections between these and the academic partners.

PLANNED PROJECTS

In order to best represent and investigate the opportunities and challenges of the wide span of IoT applications, the partners have created a project structure which feeds into the generic themes of interest; Privacy & Trust, Safety & Security, Harnessing Economic Value, Standards, Governance & Public Policy, and Adoption & Acceptability. A number of projects will provide evidence under these headings; these we have grouped by type or sector into areas of applications or 'Constellations'. Around 20 initial projects cover the constellation themes. PETRAS has been designed so that further internal calls for projects can be shaped to fill the research gaps identified with user partners and then consolidate the research outcomes into concrete demonstrators. PETRAS plans to become the go-to place for research in cyber security of the IoT in the UK by creating an inclusive technical and social platform for innovation that will continue beyond the end of the funded period.



INFRASTRUCTURE | IDENTIFICATION | SUPPLY & CONTROL SYSTEMS | AMBIENT ENVIRONMENTS

Examples of projects within these constellations include: **Transport & Mobility** where projects will include smart street planning, pricing and road maintenance, and security and privacy solutions for communicating autonomous and semi-autonomous cars and infrastructures. The **Health & Care** constellation will include modelling and analysis for body sensor networks, security mechanisms for miniaturised low power chips, and an investigation of the factors of user trust in medical applications of IoT. **Design & Behaviour** explores the role Design plays in influencing the adoption of IoT. In particular, how Design and Engineering can actively encourage or discourage behaviours, so that Privacy and Trust are enhanced and adoption is promoted. Projects under the **Infrastructure** heading look, from a policy angle, at approaches in various countries and across borders to manage IoT threats and increased attack surfaces. These projects include tools to analyse threats in many contexts. **Identification** constellation projects deal with the trustworthiness of identification systems and evaluating identification technologies, protocols, and procedures alongside privacy strategies, to identify robust solutions that deliver a balance between identifiability and privacy of IoT technology. **Supply & Control Systems** projects cover secure IoT-augmented control systems for industry and buildings, and exploring the economic value of IoT data in cyber physical supply chains. The **Ambient Environments** constellation investigates the impact of security on adaptability within cross-layered network wide protocols for low powered IoT devices. A combination of 'In the Wild' experiments on the Olympic Park and focus groups will explore the boundaries of privacy, trust and personalisation.

Further information can be found on the PETRAS web-site: www.petrashub.org

EMPLOYEES BEHAVING BADLY?

DEBI ASHENDEN

Most of the literature on insider threat focuses on either the 'malicious' insider or the 'accidental' insider. But what about those individuals who know what they should be doing but choose to deliberately breach security because they think it's in the interests of their organisation?

I've started calling these 'everyday insider threats'. Industry reports tell us that employees often admit to breaching security because it 'gets in the way.' A significant proportion of these individuals also believe that they won't get caught. These are deliberate but not necessarily malicious acts. They are often small individual actions that unfortunately have the potential for significant organisational impact.

IRRATIONAL BEHAVIOUR

Traditionally, security research has taken a rational approach to understanding the insider threat. This approach features in the Simple Model of Rational Crime and also in broader theories such as the Theory of Planned Behaviour and the Theory of Reasoned Action. The assumption of these theories is that employees consider the potential costs (will I get caught?) against the potential benefits (what will I gain?) before misbehaving. Such a perspective has merits. We know from research that, under some circumstances, offering financial (or other) incentives along with priming on possible consequences, supplying extensive feedback, and giving training, can deter people from breaching security.

However, it doesn't work reliably. What seems rational to the expert manipulating the cost/benefit exchange isn't always rational to the individual carrying out the behaviour. There are other factors at play, and thresholds to costs and benefits vary across individuals. The rational approach may also be used to offload responsibility. The security practitioner argues, 'but we told them why they shouldn't do it,' and the employee responds, 'but I couldn't do it any other way'. Finally, what works in a lab when such a cost/benefit exchange is negotiated doesn't always work in the real world. Things are more complex.

It seems that good people can do bad things and, unfortunately, what looks like rational behaviour to one person (the security practitioner) does not to someone else (the employee). So what's really going on here and is there something we can do about it?

There is a wealth of research on the concepts of workplace deviance, counterproductive workplace behaviour and organisational citizenship behaviour. Workplace deviance and counterproductive workplace behaviour are intentional behaviours that cause harm to the organisation. Organisational citizenship behaviour is voluntary behaviour that benefits the organisation. These three kinds of behaviour are linked but the first two are not opposites of the third. An employee can do both, or do one when they think that they are doing the other.

LOAFERS, FREE-RIDERS AND SUCKERS

There are at least three possible explanations coming out of research that might explain why employees do what they do. The first possibility is 'social loafing'. Individuals hide in the crowd and think that nobody will notice their limited contribution, or that they're breaching security. The second possibility is the 'free rider effect'. Individuals perceive that their misbehaviour doesn't matter because sufficient people are doing the right thing. In security terms this might be when there is a reliance on the technology or business processes to deliver security rather than the actions of an individual employee. The third possibility is that employees don't want to be seen as 'suckers'. They see others breaching security and conclude that if others aren't complying then they don't need to either.

Good people can do bad things and unfortunately what looks like rational behaviour to one person (the security practitioner) doesn't to someone else (the employee).

Fortunately, there are interventions that can help organisations counter all three of these assumptions. Ensuring employees know that their actions can be identified, giving them feedback on a regular basis, and presenting compelling evidence that their contributions are important, have each been shown to help. As has enabling employees to compare their behaviour with those of others, since it decreases social loafing. Finally, encouraging group cohesiveness can also help to ensure employees are given opportunities to help each other, though the effects of this has yet to be explored in a security context.

SPENDING BROWNIE POINTS

So that's the problem of the 'everyday insider threat' solved then isn't it? Unfortunately, it's not that straightforward. Individuals can be tricky and again, while these interventions will help in certain circumstances, there are instances where research has shown they won't work. For instance, it seems that good deeds by an employee can mean that she or he feels entitled to act badly in the future. The greater the reward for compliance the more 'naughty' it can feel to not comply. Moreover, organisations like their employees to be creative and innovative but these traits are often positively associated with misbehaving. Thresholds for how employees can misbehave and yet still feel good about themselves vary a lot.

It seems, then, that there's good news and bad news. While the interventions outlined above are a good starting point, they can't be relied upon to work every time. These interventions also give us an interesting research proposition – how much will people 'cheat' at security and under what conditions? How can we better understand the trade-offs that employees make and what is really happening underneath the mandated processes and policies? Can we improve security by, rather counter-intuitively, making people jointly responsible for compliance rather than individually responsible? These are the questions that the Protective Security and Risk programme of CREST are addressing.

To find out more about this research visit the CREST website (www.crestresearch.ac.uk).

EVERYDAY SECURITY: A MANIFESTO FOR NEW APPROACHES TO SECURITY MODELLING

RENÉ RYDHOF HANSEN
AND LIZZIE COLES-KEMP

THE IMPORTANCE OF EVERYDAY SECURITY

'Everyday security' describes the ability of an individual to go about their digital activities with confidence and trust. The importance of everyday security in the delivery of government services has greatly increased over the last decade. For example, the UK government's *'digital by default'* agenda sets online service delivery as the primary mechanism for implementing essential civic services, including housing, employment, education, healthcare, welfare, transport, food and criminal justice services. These are provided by central government departments that support the *digital by default* agenda. Consequently, the majority of UK households digitally access essential civic services, with some of the largest increases in digital access occurring in low income households. The everyday security needs of such a diverse user community are highly varied but the design of service security is often unresponsive to this variety. This results in parts of society being unable to comply with the security requirements of the service.

One example is the use of passwords to access essential services. Whilst much focus in internet safety is on 'one user-one password', the reality is that many service users rely on 'social proxies' (other people such as carers, family and friends) to help them login and administer, for example, health, welfare, employment and housing services. So, the digital service security question is not so much one of secure passwords but more one of enabling the individual to manage their social proxy and to be able to detect if that social proxy begins to work against their interests.

MANIFESTO FOR EVERYDAY SECURITY MODELLING

In order to respond to these challenges, the underpinning models and philosophy of service security need to be re-designed. We need to understand what needs to be secured, and then what security means in this context. We also need to design for the conflicts that emerge between service stakeholders. This requires techniques for modelling that accommodate the goals of security whilst acknowledging that these may change over time.

Such modelling would be in contrast to traditional models that rarely scale well and usually do not have effective means of modelling implicit, inconsistent, or contradictory goals. Whilst we're good at designing the possible and necessary security features of a system, our traditional approaches do not typically respond to the needs of everyday security. This is, in part, because traditional models focus on capturing and reasoning about protection of information and computing assets.

The security philosophy of everyday security also differs to the security philosophy that informs traditional security. This is because the focus of traditional security design stems from the security concerns voiced by the technological and policy security communities. As the social proxy example shows, these concerns are at times misaligned with the concerns related to the everyday security experience of citizens.

INTRODUCING A FAMILY OF MODELS

Recent research suggests that a family of security models (and modelling processes) are needed to respond to both system and everyday security concerns, starting with exploratory models and moving to more classic, mathematical models once the goals, conflicts and inconsistencies are defined. At the same time a transformation in security management practice is required. This means that together with the more traditional, mathematically-informed approaches to risk assessment and audit, approaches from design and the humanities that encourage active and reflective end-user participation and engagement are needed. Including such participation in security management approaches will help stakeholders identify conflicts and ambiguities in the service design. Such a family of modelling techniques provides a landscape in which interdisciplinary teams can work together—both in academia and in practice—to leverage the strengths of each discipline and respond to the complex problem of everyday security.

ABOUT THE AUTHORS

René Rydhof Hansen is a computer scientist and an associate professor at the University of Aalborg. Lizzie Coles-Kemp is a professor whose work focuses on the social aspects of information security at the Information Security Group, Royal Holloway University of London.

TIM STEVENS, KINGS COLLEGE LONDON

CYBER SECURITY AND THE POLITICS OF TIME

Tempus fugit, the Roman poet Virgil reminded us, an observation that seems more apt with every passing year. We are living through the 'Great Acceleration' in human activity, precipitated by the 18th-century industrial revolution and catalysed by the information revolution of the present. Caught up in the webs of globalisation and computerised high-technology, we feel more than ever that 'time flies', as we struggle to keep up with the pace and scale of change. Few feel this more acutely than policy-makers and legislators confronted with the practical challenges of managing societal change in the national and global interest.

Cyber security is one field in which those charged with protecting populations are seemingly always playing 'catch-up' to the global information environment. Such is the dynamic evolution of malicious software, the diversification of cyber crime, and the proliferation of state cyber espionage and cyber warfare capabilities. Any attempt to regulate these phenomena appears a thankless and impossible task. And yet, against this backdrop, there is ample time for reflection and deliberation on what cyber security policy and strategy is required. There is no need to panic or to pursue ill-judged policies in response to the rapidity of global change. Indeed, being seduced by this speed and acceleration is the worst possible basis for drafting and implementing policy in pursuit of positive cyber security gains.

To understand this, we must appreciate there is no single time at work in the world but many. Multiple actors and processes operate at varying speeds and on different time scales and therefore make political and practical calculations at variance with those of others. In cyber security, for instance, computers work at fractions of time incomprehensible to humans, which is why we delegate tasks that require split-second responses to machines physically capable of making them. This automated software and hardware, and 'smart' systems, learn and adapt to stimuli and situations but are essentially 'dumb'. Cyber security specialists act as interfaces between these systems and the environment. They need to make rapid decisions, for sure, but their human temporality is a time for shaping the rules by which these technological systems act, not for interfering directly with the millisecond decision-loops of computers themselves.

At another temporal level again are policy and strategy. In democracies, policy-making occurs in institutional contexts of more attenuated deliberation and negotiation. While this might seemingly frustrate progress on key issues, such as public-private information sharing, there is no evidence policy made in haste is any better than policy crafted by slower means. The opposite is true: such is the significance of contemporary developments that we should be thinking longer and more carefully about how we tackle cyber security. Instead of rushing to keep up and being captured by narratives of the 'tomorrow is too late' variety, we need to think longer-term about the role that cyber security should play in our future. This might take two principal forms, one facilitating the other.

Societies need to determine what cyber security is for in the short- to medium-term and enable it in intelligible and socially productive ways. This requires a recalibration of what is of social value, not necessarily only what is of immediate national security or corporate interest. At present, we give too little consideration to the needs and rights of citizens, and too much to the demands of security agencies and big business. These constituencies are essential cyber security actors but the public good should be the principle that guides the allocation and investment of resources and the ethics and practices of cyber security professionals both public and private.

Building on this, our second concern must be with what cyber security will do in the long term. What sort of future world do we want? How do we secure a hyper-connected population and economy? What does security mean in the 'Internet of Things' or in 'smart cities'? How is privacy being reconfigured and what does this mean for society? Must we prioritise cyber-enabled surveillance as means of regulation and control, or can we imagine ways of enabling citizens to pursue their legitimate desires and goals? It would be incorrect and unjust to say that governments are not beginning to think through and consult on these issues, but much more needs to be done.

This much may seem obvious but the value of thinking about the temporal aspects of the politics of cyber security is twofold. It is essential to recognise that there are different time scales for the different actors in cyber security, from computers to citizens to government and international organisations. We should, of course, seek to reduce bureaucratic torpor and institutional inefficiency, but some distance between action and reaction can be a resource for improvement, not despair. For example, in the case of a major cyber attack causing infrastructural degradation and human harm, a rapid reaction should be reserved for responders not foisted on policy-makers. They must be encouraged and allowed to form policy that addresses the future, not over-reacts to the past.

Another valuable aspect of a more temporally sensitive approach is the recognition that neither time nor policy stands still. The politics and practices of security are constantly changing and we should embrace that instead of lamenting it. There is no perfect cyber security solution now, nor will there ever be, but there is a place for well-thought out policy. This will require courage on the part of policy-makers and no small degree of bipartisanship. The obstacle to good policy is not the speed or acceleration of the information age but the willingness of humans to work together for the public good. If politics is about visions of the future, there can be few more pertinent illustrations of this than cyber security.

CYBER CRIME AND THE SOCIAL WEB

PETE BURNAP AND MATT WILLIAMS

Many of us spend significant amounts of time on the 'Social Web', the human-centred interactive ecosystem made up of mainstream and social media as well as interactive blogs and websites. However, emerging alongside the innovation that drives these new networks are equally dynamic cyber crime threats that challenge traditional approaches to policing. Criminal activity on the Social Web represents a new frontier for national and international security and crime fighting, yet such interactive spaces remain largely unregulated. Given the scale, international reach and open nature of the Social Web, law enforcement agencies struggle to meet an expectation of protection from the public.

Cyber crime can be thought of as both cyber dependent – crimes that require information and communications technology in order to be executed and cyber enabled – crimes whose scale or reach is increased by use of computer networks or other internet platforms. In the case of cyber dependent crime, Kaspersky Labs and Symantec anticipate a rise in cyber attacks conducted via social media. Examples of the cyber crimes emanating from this include denial of service attacks, phishing attacks and malware for the commission of network intrusion and cyber fraud. These crimes are an increasing problem for law enforcement agencies. We are seeing social media being increasingly adopted as a dissemination mechanism for hate speech and inciteful content. Both are unlawful in the UK and pose a threat of social unrest within communities, which has been linked to extremism and radicalisation.

For policing purposes, having intelligence on whether cyber threats are escalating or deescalating in frequency is crucial. Research into the quantification of these cyber and human factors has been the core objective of our work over the past 3 years. We have developed algorithms to classify and measure online reactions, and predict emerging threats to cyber (malware attacks) and human security (antagonistic social content) using data mining, machine learning and statistical modelling.

Criminal activity on the Social Web represents a new frontier for national and international security and crime fighting, yet such interactive spaces remain largely unregulated.

Online social networks (OSNs) (e.g., Twitter, Facebook, Tumblr) are inherently vulnerable to the risk of collective contagion and propagation of malicious viral material such as malware and antagonistic content following widely publicised emotive events. Our research on cyber hate following the attack on Drummer Lee Rigby found that it spiked for up to 36 hours on Twitter following the attack, dropping sharply after this period. We also found that it was possible to identify that the longest surviving narratives surrounding the attack were from the police, and far-right political groups. This type of measurement offers significant value to those seeking to observe and monitor levels of cyber hate in the immediate aftermath of a 'trigger' event, such as a terror attack.

We have also studied the behaviour of web links posted to Twitter during the Superbowl, Cricket World Cup, and European Football Championships, with the aim of identifying URLs that perform 'Drive by Downloads'. These occur when the URL endpoint is a server that contains a malicious script which, when executed, attempts to exploit a vulnerability in the browser or a plugin to perform malicious activity on the user's device. A prominent example of the injection of malicious URLs into OSNs is the Koobface worm. Koobface initially spread by using an infected machine to send messages to Facebook 'friends' of the infected user, which included a link to a third-party website that infected the machine of the user visiting it by installing malicious software. The worm was effectively executed on a number of OSNs due to the highly interconnected nature of these network's users. Research identified that current defences flagged only 27% of threats and took 4 days to respond. During this period, 81% of vulnerable users clicked on Koobface links. This highlights the requirement for real-time accurate classification of malicious URLs to limit the infection rate and damage inflicted on global IT infrastructure.

As the Social Web evolves policing authorities will need innovative and automated methods to successfully observe and manage dynamic, large-scale threats emerging from cyber criminals. In the UK, the government have ramped up efforts to tackle cyber crime in a collaborative way through a new National Cyber Security Centre, and the Metropolitan Police force has recently announced that it is to set up an 'Online Hate Crime Hub' to target online Hate Crime. These initiatives offer public and private-sector researchers the opportunity to develop the technological and interpretive techniques necessary to maximize the effectiveness of these national strategic centres. At the same time, ethical observation and the upholding of a fundamental principle of the Web, that 'it is for everyone', is absolutely necessary for the balance between appropriate policing and freedom of expression.

As the Social Web evolves policing authorities will need innovative and automated methods and infrastructure to successfully observe and manage dynamic, large-scale threats emerging from cyber criminals.

Dr Pete Burnap and Professor Matt Williams direct the Social Data Science Lab at Cardiff University. This is an Economic and Social Research Council (ESRC) 'Big Data' programme that brings together social, computer, political, health, statistical and mathematical scientists to study the methodological, theoretical, empirical and technical dimensions of new forms of data in social and policy contexts. Learn more about their research at http://socialdatalab.net

MARCUS K. ROGERS, PURDUE UNIVERSITY

HACKER MIND SET

The term hacker has become a common word in our vocabulary. Few people have never heard of the term and almost everyone believes they understand what it means. Yet, despite almost 20 years of research into the motivations, psychological characteristics and mind set of hackers, we really know very little. The research to date indicates that there is no 'one size fits' all generic hacker profile. Hackers are as diverse as any other criminal category or deviant grouping. While the underlying common denominator that separates hackers from other categories is the use and/or targeting of technology to commit some deviant or criminal act, that is where the uniqueness ends.

The motivations driving hackers to commit their crimes runs the gambit from greed, revenge, desire for notoriety, to patriotism and psychopathologies. Part of the reason for this wide continuum is the fact that hacking encompasses activities and subcategories that, according to the most recent research, evolves with the technology and society's comfort with and use of technology. We now have subcategories of hackers that include political activists (Hacktivists), criminal organisations (e.g., Anonymous), organised crime, and state sponsored/cyber warfare (cyber operations). People now have the ability to purchase ready-made attack tools that can be customised for the target, and require nothing more than the click of a button to carry it out. Additionally, our society is now a globally connected society with access to information 24/7, and the ability to see what people are doing almost every minute of their lives based on their social media postings.

... there is no 'one size fits' all generic hacker profile.

It is no wonder that researchers have struggled to identify common psychological profiles and motivational patterns in order to help better defend our cyber infrastructures and our own personal data. The creation of customised attack tools complicates studies that attempt to profile hackers based on real time activities, as it is uncertain whether one is measuring an automated tool or a real person.

Given the limitations of the research and the herculean task of trying to deal with all of the potential confounding variables, it would appear that hackers (other than state sponsored) are motivated primarily by greed, revenge or desire for attention. The research also indicates that with 'lone-actor' hackers there is usually some kind of critical path and trigger events that push the individual from thinking about attacking systems, to actually carrying out the attack. These trigger events can be unique to each individual but the event will cause a stress reaction that seems to push the individual over the proverbial edge.

The mind set of hackers that come together in groups such as hacktivists and loose criminal organisations, centres more on revenge and/or notoriety. These groups are more methodical in their choice of targets and their targets are typically symbolic in the case of hacktivists, or somewhat strategic in the case of the criminal organisations (e.g., rival groups, soft targets).

The remaining category of state sponsored and/or cyber warfare (AKA cyber operations) is not a unique deviant or criminal organisation. These individuals are part of the larger espionage world or military and are operating under direct (if not indirect) orders from their country. The mind set of these individuals is better understood in terms of military doctrine and patriotism.

While hacking is an artefact of technology and our connected society, much more work is needed to try and not just understand their mind-set (albeit subdivided into the various sub-categories) in order to deal with current threats, but to try a predict what will happen in near term future. The holy grail of research into hacker psychology is the concept of cyber adversarial predictive analysis; what are they going to do six months, one year, or five years down the road. But for now that seems more like science fiction than science reality.

JOANNE HINDS

What is the role of technology in an emergency?

Emergencies are unpredictable, rapidly changing events that require the co-ordinated efforts of professional responders with victims on the ground. In the last 18 months, such events have included the Nepal earthquake, Typhoon Soudelor in the Philippines, as well as several terrorist attacks. Each disaster is unique, and attempts by professional responders to prepare are inevitably limited by our capacity to anticipate the scale, scope, location and people affected are often unanticipated. However, one aspect that can be anticipated is the importance of a 'technological response', where people turn to the internet for information and to provide support. Here are some of the main uses for technology in a disaster.

CROWDSOURCING INFORMATION TO HARNESS 'COLLECTIVE INTELLIGENCE'

Crowdsourcing applications such as Ushahidi can help to accurately depict circumstances by pooling people's efforts. Ushahidi first came to light during the eruption of violence following the 2007 presidential elections in Kenya. Kenyans used Ushahidi to text reports of the violence from their mobile phones. The reports were added to an online map and within a matter of days the crowdsourced efforts obtained through Ushahidi had obtained a more complete picture of the violent activity than any other organisation.

CREATIVE RE-PURPOSING OF EXISTING APPS AND SOCIAL NETWORKS

During the 2010 Haiti earthquake Dan Wooley was trapped under some rubble. By using a medical app on his smartphone, he successfully treated his injuries using his shirt and belt, aided by the phone's torch. By setting his alarm to go off every 20 minutes, he was able to sustain his condition until he was rescued 60 hours later. Other creative uses of existing technology are used by groups. During the Virginia Tech shootings in 2009, students quickly established the Facebook group 'I'm Safe at VT', where people reported their whereabouts. The accuracy of the information meant that they unintentionally determined the names of the deceased before they were officially released.

COMPENSATING FOR THE FAILURE OF TRADITIONAL COMMUNICATION TECHNOLOGIES

Whether through physical damage or a surge in use, one of the most common problems that arise during emergencies is that communications networks fail. FireChat is an example of a smartphone application that can operate in the absence of a Wi-Fi or mobile phone connection. It operates via a Bluetooth mesh network, which means that as opposed to traditional messaging services, the more people use it, the better it works. One of the first widespread uses of FireChat was during the Hong Kong protests in 2013, where protestors used it to organise and mobilise activities.

EMPOWERING REMOTE SUPPORT

Just as news of a disaster can rapidly spread throughout the world, those wanting to provide remote assistance can easily do so by sharing information online. Some organisations bring together volunteers to co-ordinate their activities online. For example, The Standby Task Force is a global network of volunteers who collaborate during disasters by completing numerous online activities including mapping, research and a variety of Emergency Management tasks.

FUTURE DEVELOPMENTS

Social scientists are studying these kinds of interactions in the relatively new field of Crisis Informatics, which is the study of the use of technology in disasters and emergencies. Some examples of future developments coming out of this research include:

Identifying users through different patterns of activity – Users remote from a disaster tend to generate the majority of information about it. However, users local to the scene differ in the type of content they broadcast online. They often act as a source of information and they tend to share other locally-created information. The ability to distinguish between local and remote users is useful when determining the trustworthiness and accuracy of information, and when prioritising aid and rescue.

Using social media to understand socio-behavioural phenomena – Retrieving and analysing online behaviour provides insights on how groups share information and self-organise. Studying what types of online behaviour successfully improve response efforts has helped researchers develop computational tools to encourage beneficial behaviours in future crises.

Establishing effective communication methods for emergency responders –Emergency responders face a number of challenges in using social media and other online tools. Any unclear or inaccurate information may have serious consequences if people take the wrong action as a result of such information. It is also still the case that command and control procedures lack policies for social media usage. By studying the ways emergency responders use social media, researchers seek to inform and improve future policies for emergency response.

A HINDRANCE OR A HELP?

While technology can help emergency response efforts, there can also be problems with using the vast amount of information available. For instance, it can be difficult to determine which information is correct or true. Rumour can easily spread, causing issues with trust, and decisions based on inaccurate or false information can have damaging consequences. In some cases, public access to information on social media can be used to incite violent behaviour. The limitations and opportunities provided by technology vary according both to the particular situation faced and the new patterns of online behaviour as people discover new ways of collaborating and communicating.

What the current research and the examples listed above show, is that whether it is a hindrance or a help, technology does now have a central role to play in responses to emergencies.

The limitations and opportunities provided by technology vary according both to the particular situation faced and the new patterns of online behaviour, as people discover new ways of collaborating and communicating.

Joanne Hinds is a CREST Researcher, based at the University of Bath.

Expanding the frontiers of interrogation research and practice

The US government's High-Value Detainee Interrogation Group uses science-based, ethical, and rights-respecting methods of interrogation. Christian A. Meissner, a professor of Psychology at Iowa State University and Susan E. Brandon, research programme manager at the HIG, have been responsible for coordinating an unclassified interrogation research programme that puts these evidence-based techniques at the heart of training and practice.

While interrogators have successfully collected criminal evidence and human intelligence for decades, the methods used have at times brought about the collection of false confessions and misleading intelligence information. In fact, a 2006 Intelligence Science Board study concluded that the US government's interrogation practices were largely devoid of any scientific validity (see 'Improving practice through research' in CSR issue 1). To address this issue, the Obama administration established the High-Value Detainee Interrogation Group (HIG) in 2010. In addition to its operational mandate, the HIG was tasked with creating an unclassified program of research to evaluate best practices in lawful interrogation.

Since that time, researchers from the US, Europe, Australia, and elsewhere have been working to identify and test the most effective means of acquiring intelligence and gaining cooperation from interviewees. The resulting research has produced studies ranging from laboratory experiments, to interviews and surveys of interrogation professionals, to systematic analyses of actual criminal and counter-terrorism interrogations.

With more than 100 publications stemming from the first five years of the research programme and additional new research projects underway in 2016-17, a parallel training programme is enabling practitioners in law enforcement, the Defense Intelligence Agency, the FBI, and the CIA, to work directly with researchers to embed their findings and best practices into day-to-day operations.

THE SCIENCE OF INTERROGATION

The emerging science of interrogation relies on a variety of disciplines and fields of study for its theoretical and scientific foundation (from criminal to clinical interviewing), many of which have offered a foundation of research to build upon.

In fact, research on interviewing and interrogation in the criminal justice system has been steadily accumulating since the 1960s, providing data on topics such as effective and ineffective elicitation methods, the conditions under which victim, witness and suspect memories are most vulnerable, valid cues to deception, and factors that lead individuals to confess to crimes that they did or did not commit.

During the same period, a scientific understanding of principles leading to successful negotiation and social influence (persuasion and resistance) also began to emerge. Together, these and other research areas provide a foundation from which the HIG began to support research aimed at developing a more effective, ethical, and science-based model of interviewing and interrogation.

BUILDING MODELS OF INFORMATION-GATHERING

The science developed by the worldwide team of researchers over the past six years consistently reveals that rapport-based, information-gathering techniques produce the most accurate and comprehensive information. Those that have been identified as fundamental to effective and ethical interrogations are described in a report to the US government, due for publication in early 2017, that focuses on using rapport-based methods for developing cooperation and countering resistance, applying the most effective methods for eliciting valid information from memory, and facilitating assessments of credibility with strategic interview methods.

The science developed by the worldwide team of researchers over the past six years consistently reveals that rapport-based, information-gathering techniques produce the most accurate and comprehensive information.

Based on empirical data, these researchers propose a good practice model of interrogation as a dynamic process in which interrogators must engage in 'sensemaking', in which they continually evaluate the cooperation and resistance offered by a subject. The interrogator must develop and sustain rapport by allowing the subject a sense of autonomy, showing acceptance, adaptation and empathy, and drawing out the subject's beliefs, motivations, and concerns. Influence strategies and 'priming' are also likely to be important for improving cooperation and furthering rapport. When the subject is willing to talk and engage on a topic identified by the interrogator, the information collection method must build on what is known about the processes of memory, social dynamics and communication – using methods such as the Cognitive Interview, Observing Rapport-based Interpersonal Techniques, and the Scharff Technique (you can read more about all of these methods at www.interrogationscience.org). The information that is elicited – both about past events and intentions for future actions – should be consistently checked for validity, using cognitive-based cues rather than anxiety-based cues.

By integrating operations with research and introducing science-based methods into formal training programmes, the HIG is advancing the science and practice of interrogation, helping the intelligence community to better evaluate what makes a good interviewer, to consider new approaches to gaining information from criminals and terror suspects, and to use evidence-based methods to detect deception.

*Read more about findings from the HIG-commissioned research at **www.interrogationscience.org**.*

Loyal footsoldiers – the attractions of EDL activism

ELIZABETH MORROW

Islamophobia is widespread in the UK. A 2015 YouGov poll found that over half of British voters think there is a fundamental clash between the values of Islam and British society. Despite Islamophobia entering the mainstream, most people who sympathise with it will not participate in protests organised by groups such as the English Defence League (EDL). With such a deep pool of potential participants, why is anti-Muslim protest not more common?

This puzzle can be solved if Islamophobic activism – like other forms of political organisation – is understood as a collective action problem. Because the benefits of political action may be enjoyed by participants and non-participants, whereas the costs are borne by participants alone, it may be in an individual's self-interest to free-ride on the activism of others rather than directly participate and bear the costs of political activity. One way in which a political organisation may overcome the collective action problem is through the provision of club goods to participants that cannot be enjoyed by non-participants.

Photo by Gavin Lynn / CC BY 2.0

In the case of the EDL, those who engage in organised Islamophobic activism do so because participation brings direct personal benefits that outweigh the personal costs. Throughout 2013-2014 I conducted fieldwork with the EDL, and attended a number of EDL demonstrations, 'meet and greet' events, informal pub gatherings and was added as a member of a closed Facebook group. This original data reveals that the participation of grassroots members was driven by the club goods of access to violent conflict, increased self-worth and group solidarity. These goods are supplied exclusively to EDL members; that is, they could not be obtained other than through EDL participation.

In his study of the EDL, Joel Busher found that 30-40 per cent of EDL members were football hooligans, and notes that physical confrontations with opponents were an essential element of the EDL's 'emotional alchemy'. In research I conducted with John Meadowcroft, we similarly found that a striking feature of the EDL was the important role of violence within the organisation, and that participating within the group gave members an opportunity to engage in physical altercations. For example, at a demonstration in the centre of Birmingham in July 2013 numerous scuffles between EDL and Unite Against Fascism counter-protestors were witnessed and a number of EDL members came away bleeding from head wounds. EDL members were observed sniffing and eating a white powder before moving to the front of the demonstration to aggressively taunt police and counter-demonstrators. Accordingly, we conclude that EDL street protests are likely to appeal to football hooligans because of the opportunities for violent conflict at these events.

EDL participation also enables members to construct a sense of self-worth that affirms their dignity independently of their low socio-economic status. We found that EDL activism is couched in moral terms – particularly, the duty to protect one's family and one's community – that provides its predominantly working-class members with a heightened sense of personal self-worth. For example, during the Birmingham demonstration, one member revealed that he thought his family could be protected by his EDL participation when he stated that '[David] Cameron won't stand up for us,

A striking feature of the EDL was the important role of violence within the organisation... participating within the group gave members an opportunity to engage in physical altercations

so we have to stand up; if we don't stand up, it will be my children, and I'd rather it be me than my children'. EDL membership also increases self-worth by purportedly providing participants with an opportunity to protect their country. Indeed, EDL participation is presented as analogous to being a soldier of war. The very name 'English Defence League' connotes quasi-military action to safeguard the country against Islam. Many EDL members (both men and women) wear branded clothing that states their division, emblazoned with the words, 'Loyal Footsoldier'.

The third exclusive benefit that the EDL supplies to its members is group solidarity: the opportunity to be part of a close-knit group united by the belief that they are fighting for a common and just cause. For example, at one meet-and-greet session an EDL member told the audience that when they go to a demonstration, 'you go as brothers and sisters'. He talked about getting the coach to an upcoming demonstration, and said that when members travel on the coach they 'are like a family', and told them 'you have to respect that you will be travelling as part of a family'.

As well as the benefits described above, like all political activity, EDL membership also imposes costs, in particular, stigma. Indeed, it is such a stigmatised activity that several members revealed that they had family and friends who privately supported their activism, yet did not want to participate more actively because it might jeopardise their career. One member revealed that although he had managed to persuade his mother that the EDL 'isn't bad or racist', she was unable to 'support him officially' because she would lose her job as a teacher if her support became public. The same member also said he did not fear losing his job because he thinks that his managers at the warehouse are supportive of his EDL involvement, yet 'can't say so out loud because they'd be sacked'. This data strongly suggests that EDL sympathisers will not turn to activism if the cost (in this case, job loss) exceeds the benefits to be gained from activism. It is also worth noting that these examples suggest individuals with jobs that place them in the public eye – for example, teachers and managers – are more likely to face employment sanctions than those with less visible occupations.

The benefits of EDL membership will appeal more to those individuals who enjoy violence and aggressive confrontation, have low self-worth and value the group solidarity the EDL offers. Accordingly, it should not be surprising that most EDL members are young men, often with links to football hooliganism, who are employed in industries that are unlikely to sanction them for their involvement. To understand the appeal of EDL activism, it is not enough to examine the group's ideological appeal; the costs and benefits of individual activism must also be identified.

Dr Elizabeth Morrow is a CREST Researcher based at the University of Birmingham. This article originally appeared on Radicalisation Research, an online resource for academic research on radicalisation, extremism and fundamentalism. You can read the original article here: http://www.radicalisationresearch.org/debate/morrow-2016-loyal-footsoldiers/

LINDA WOODHEAD,
LANCASTER UNIVERSITY

THE CONTINUING GROWTH OF RELIGIOUS EXTREMISM, AND HOW TO COUNTER IT

While many people have observed that religion is in decline in some parts of the world, less have noticed that the nature of religion has also been changing – especially since the 1980s. What we have been seeing is a gradual 'hardening' of religion, with more extreme, fundamentalist forms growing in influence, and more moderate, mainstream forms declining. Why has this happened, and could it be that legislators, inspired by an ideal of 'religious freedom', have unwittingly been complicit?

EXTREMIST VERSUS MODERATE RELIGION

I use the words extremism, fundamentalism and sectarian or illiberal religion to refer to the same phenomenon. Religious extremism is of course not the same as violent religious extremism, which is a small subset of it. Synthesising a massive amount of research on the phenomenon, we can define it as that form of religion which maintains that:

1. there is only one body of truth (deriving directly from God/a higher being),
2. that only one particular group has access to this truth
3. that the truth can be stated in clear, fundamental propositions
4. that all who disagree and disobey are enemies of God.

THE DYNAMIC OF EXTREMISM

My characterisation of extremist religion would meet with quite wide agreement amongst scholars of religion. What is not yet as widely accepted, but what I believe to be supported by the evidence, is that there is, in every monotheistic religion, an extremist dynamic which operates so long as nothing – such as the countervailing force of moderate religion, or government intervention – checks it. This extremist dynamic operates for a number of reasons.

First, ambitious individuals setting themselves up as religious leaders can always purify a religion a bit more and there is always a motive to do so: the people who set themselves up as the purifier claims to be more obedient than the rest, he is a more courageous defender of costly truth. He can then make a power grab, perhaps through schism.

Second, extremists can never go backwards/liberalise and say they were wrong, because they claim to know the truth, a truth which is unchanging. To admit fallibility brings the whole thing crashing down, and with it one's own authority - it all hangs or falls together.

Third, to prove themselves obedient, fundamentalist followers have to follow: when the leader says jump you are meant jump – even to the point of death. A few really will. So well-organised fundamentalist religion is often more immediately effective than liberal forms of religion, which have to broker agreements and cannot simply order people to obey.

Finally, opposition is confirmatory, it just proves that the group is right – the fact that 'the world', the 'secular authorities' and moderate religion ('the liberals') oppose them is what they need and expect. Extremist identity is created in conflict and depends upon it.

MODERATING FORCES

In much of history the extremist dynamic does not take over in a religion because it is checked by moderating forces. These forces can be internal (push back from moderate majorities and leaders) and external (e.g., political rulers' patronage of moderate forms, and opposition to extremist forms). Although the moderating forces will differ according to the religion, a country and its history and constitution, we can identify a number of important moderating elements. These are particularly effective when the 'secular' power has legitimacy with the populus:

- Some system of state support, oversight, or funding (e.g., religious establishment and parliamentary oversight of the Church of England; state funding of the churches in countries like Denmark and Germany).
- Strong ties which bind religion to wider society, and entry points into that society, e.g., in relation to schools (good RE, moderate faith schools), hospitals (chaplains), or everyday life (e.g., religious weddings and funerals as a norm).
- A good relation between religion and mainstream education (e.g., religious leaders are trained in universities, have a high level of education; and good RE is taught in schools to all).
- Clergy do not dominate a religion; there are forums and institutions for lay decision-making; ordinary religious people's views are represented and taken seriously; clergy serve lay people rather than vice versa.
- Women have real power in the religion, and men cannot dominate them.
- Transparency in how religions are led and run; accountable religious leaders. Good relations between religious and political leaders and leaders in civil society.
- Moderate forms of religion are respected and protected by society and state, and extremist bids for power are not aided and supported.
- The natural churn, change and evolution of all religions is respected and religion is not fossilised by taking seriously the claims of conservatives that religion and its institutions are just as they say, and are unchanging.

EXTREMIST DRIFT IS NOT JUST ISLAMIC

The growth of extremist wings in religion has been greatly aided and abetted by the fact that governments since the 1970s, not least in the West, have been too weak in countering the creeping influence of fundamentalist minorities. More liberal majorities have been sidelined and ignored.

We can see this not only in Judaism, or Islam, but in the Christian churches, both Catholic and Protestant. Since the 1970s many have abandoned a liberalising tendency and been taken over by puritanical factions mobilised for the 'traditional' (male-led) family and against equal treatment for women and gay people. Conservative leaders have strengthened their power, and liberal wings have shrunk.

In Islam the dismantling of many of the historic forces of moderation, and the failure to develop new and alternative liberal forms is also part of the background which has led not only to extremism but also to violent extremism in many parts of the world. Some of the factors include the breakdown of traditional forms of religious scholarship and the collapse of various scholarly schools and their ability to contest one another. Disruptions to traditional forms of authority and to everyday, lived 'enculturated' forms of the religion caused by migration have also played a role, as has opportunistic mobilisation around often legitimate grievances. The failure of states to support moderate Islam in effective ways, or to take early and appropriate steps to counter extremism (before violent forms emerge) is also important.

THE FUTURE OF EXTREMISM

In most religions extremism is, as its name implies, just an extreme minority position. It is hard to sustain, and moderate forms of religion which exist in a more open relationship with everyday life and society is numerically dominant. However, when the face of religion becomes increasingly extreme, moderate people vote by leaving the religion altogether. It is this phenomenon, I believe, which explains the rapid rise of 'no religion' (which is not the same as atheist secularity) in a number of countries recently. The problem is that this leaves religion to the extremists, and creates a growing tension between religion and the non-religious majority.

Paradoxically, the situation has been exacerbated by the growing influence of the ideal of 'religious freedom', according to which 'secular' authorities (including legislators) should not just leave religion alone to do its own thing, but should take pains not to interfere with 'internal' 'theological' matters, and should actively protect religious minorities. Hardline wings of religions have spotted a wonderful opportunity here. In countries which respect religious freedom they have been able to present their teaching as the 'authentic' one of the religion, and to have their position protected by law.

Even in the UK we can see this process at work. It has meant that the once moderate Church of England, for example, has been gradually dominated by its most conservative elements. Since 1975 its leaders have argued – against the opinion of most lay Anglicans – for exemptions from the law which allow them to discriminate on the basis of gender, sexuality, and religion. Parliament, which used to help govern the Church, has pulled back from 'interfering', and in the process allowed the hardliners to dominate and the moderate majority to be defeated and decline.

We urgently need to rethink the 'modern' way in which we deal with religion. Leaving religion to 'run itself' has allowed hardline leaders with much to gain and little to lose to dominate and squeeze moderate majorities. If this process is not to continue, at least three steps need to be taken. First, we need to stop treating religion as the only sphere which can exempt itself from the laws and regulations which govern other bodies and people. Second, religions and their leaders need to become transparent and accountable – to the followers and to wider society. Third, we need to become much better informed about religions and their internal parties and opinions (for example, polling of religious people is now relatively easy, and it reveals where the weight of opinion really lies). Rulers in the past knew very well how dangerous religion could be. It was the foolish modern belief that religion was, if not a benign force, at least a spent one, that led people to forget.

Opposite page: Extremist religious group protests during the 2016 Republican National Convention. Copyright Kenneth Sponsler.

FACTCHECK: THE CYBER SECURITY ATTACK SURFACE

DEBI ASHENDEN,
CRANFIELD UNIVERSITY

It isn't just your bank account criminals are seeking to access. We give an insight into the size and complexity of systems and devices that are vulnerable to attack.

1
INCREASING COMPLEXITY AND SHORTAGE OF STAFF

By 2020 there will be 35 billion devices connected to the internet, six billion of these devices will be able to request support for themselves. The amount of data on the internet will increase to 44 zetabytes (roughly the equivalent of streaming the entire Netflix catalogue more than 3,000 times). Technology fixes for security will not be able to keep up and there is a shortage of suitably qualified and experienced security staff. The qualities most valued in security staff are agility, responsiveness and trustworthiness.

2
MARKET FORCES

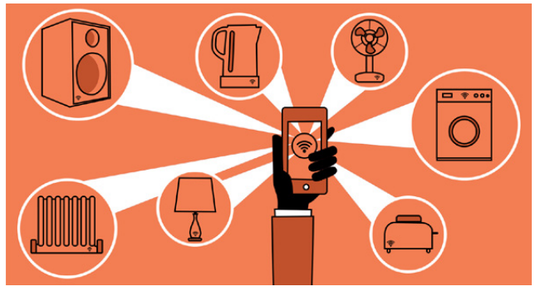
In an ideal world software would be written securely but in the real-world market forces don't allow for it. Microsoft, Google and Facebook are examples of companies that run bug bounty programmes where they will pay individuals who find bugs and exploitable vulnerabilities in their software. There are also companies, however, who trade in bugs and vulnerabilities and will sell them to the highest bidder. There are some that specialise in buying zero-day vulnerabilities (these are vulnerabilities that haven't been publicly reported previously). The highest bug bounty currently being offered is $1.5m for zero-day vulnerabilities in Apple's iOS 10 operating system.

3
INSIDER THREAT

At the moment an average large organisation can expect to see 81 million security events over the course of a year. These are alerts on a system that may or may not indicate an attack has occurred. Technology can currently filter out 11% of these. While only a proportion of these will turn out to be attacks the incident to attack ratio is rising. In the region of 55% of security breaches are caused by insiders – individuals with legitimate access to an organisation's systems.

4
INDUSTRIAL CONTROL SYSTEMS

In the US the Department of Homeland Security has said that the energy sector faces more cyber attacks than any other industry. In December 2015, the Ukraine suffered a power outage caused by a cyber attack. In May 2016, the G7 Energy Ministers highlighted their concerns about the cyber security threat to energy systems and their commitment to developing resilience against attacks.

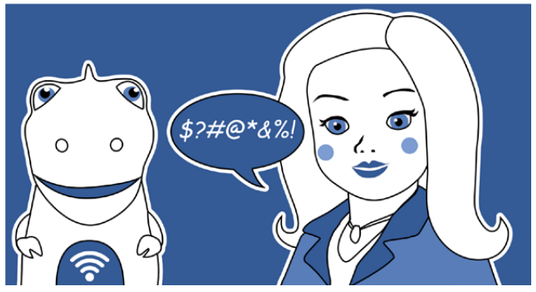


5
THE INTERNET OF THINGS

By the end of 2018, 20 percent of smart buildings will have suffered from digital vandalism. This could be in the form of attacks on digital signage, heating, air conditioning or lighting for example. The cyber attack on the US retailer Target in 2014 was through their HVAC (heating, ventilation and air conditioning). Smart buildings are often connected to the internet with weak or non-existent password protection. Physical security processes will need to be integrated with cyber security processes.

6
PERSONAL DATA

The biggest personal data breach to date is probably that experienced by Yahoo who recently admitted that names and phone numbers from more than 500m accounts had been stolen in 2014. The CEO of Yahoo apparently rejected the idea of requiring customers to change their passwords when the breach was discovered because she believed it would have an adverse effect on the business. 93% of data protection breaches are due to human error.



7
IMPACT ON FAMILY LIFE

We have seen instances of baby monitors being hacked but toys for children (such as the 'My Friend Cayla' doll) are also now wifi-enabled and speech-enabled. CogniToys Dino is a soft toy dinosaur and has advanced language processing algorithms that enables two-way speech-based interaction and uses the IBM Watson learning machine. 'My Friend Cayla' has already been hacked and instructed to recite lines from '50 Shades of Grey' and to quote Hannibal Lecter.

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 follow us on twitter **@crest_research**