SUMMER 2016 / ISSUE 01

CREST SECURITY REVIEW

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

CREST

Information Elicitation

YOUR WATCH WILL SOON KNOW YOU BETTER THAN YOU KNOW YOURSELF – p4

THE TRICKS OF MASTER INTERROGATOR HANS SCHARFF UNCOVERED – p14

SCIENCE AND THE LIE DETECTORS: WE REVIEW WHICH ONES WORK – p18

Contents

3 From the Editor

4 The future of wearable tech
Your watch will soon know you better than you know yourself

12 The promise of social science
Answering the human problems that are so central to security

16 How does memory work?
It is fallible, malleable, and hugely impressive

20 Sunni and Shi'a Muslims
One religion, two branches. Their similarities and differences revealed

24 Creativity and cyber security
Art and tech are unlikely but insightful bedfellows

INFORMATION ELICITATION

7 Eliciting information online
Why are we more trusting online?

8 Improving practice through research
What is the impact of the US educing information study 10 years on?

10 The A-Z of information elicitation
Home of one of the most valuable Zs

14 Eliciting information the friendly way
The tricks of master interrogator Hans Scharff uncovered

18 Science and the lie detectors
Lie detection techniques abound. We review which ones work.

22 Turning research into practice
The story of how the investigative interview evolved

26 Mind Map on Elicitation
We chart the lay of the evidence land

Highlights

HOW DOES MEMORY WORK?

Suggestible, transient, social and in need of our help... just how does the memory work? Lorraine Hope sets out what interviewers need to know – p16

TURNING RESEARCH INTO PRACTICE

Research has helped bring about a transformation in how police in the UK understand and use interviews. Jordan Nunan and Rebecca Milne tell us how – p22

From the Editor

We've all enjoyed watching interrogations on TV. From James Bond's painful inquisitions to Idris Elba's Luther - big physical confrontations conducted by flawed geniuses.

Thankfully, the reality has come a long way from the kind of approach epitomised by Life From Mars' DCI Gene Hunt – as Rebecca Milne shows us on page 22 where she and Jordan Nunan provide an overview into how research has helped police interviews in the UK change for the better. This is what *CREST Security Review* is all about: communicating the latest research that has, does and can inform practice and policy relating to security. Each issue includes articles on a particular focus – and our first issue addresses information elicitation.

Information elicitation covers far more than interrogation and interviewing – it occurs whenever we need to encourage somebody to provide useful information.

There are lots of techniques in this field – from using the polygraph to asking unexpected questions. Aldert Vrij and Ronald Fisher have reviewed the effectiveness of many of these techniques in real-world applications (see page 18). Emma Williams and Adam Joinson also discuss techniques that are used in methods of online elicitation.

Lorraine Hope draws on her research into human memory to show how we can support recall during interviews. Memory, she says, is not like a hard-drive where memories are stored and retrieved systematically. Instead, it's a fragile web of information and impressions that can be accessed, and shaped, by the way we ask questions.

On page 8, Robert Fein writes about the United States government research efforts to enhance expertise in eliciting information. He discusses his role in the US Intelligence Science Board's study on *Educing Information*, that reviewed, engaged with, and commissioned research on interviewing and interrogation. The programme became an engine of change for US interview practice and is an excellent example of how research can be applied to solve critical security problems.

One of the experts on interviewing during the Second World War itself was Hanns Scharff, and his ground-breaking insights inspired the research of Simon Oleszkiewicz who has investigated just what made the Scharff technique so effective. Scharff was an early pioneer of the concept of friendly interviews – where those being interrogated often were unaware of just how much helpful data they were disclosing. Our phones are similarly revealing – as Lucasz Piwek demonstrates on page 6.

We welcome your thoughts on our first issue. Let me know what you liked (or didn't), what you'd like to see in the future and if you'd like more information about the research highlighted here. Write to me at **m.d.francis@lancaster.ac.uk**

The future of... wearable technology

From mobile phones to smart watches and glasses, wearable technology isn't just the future. It's happening now. Here we show what wearable technology in general, and phones in particular, say about us and our lives. This research is in its infancy, but given how ubiquitous these devices are expect to see a lot more on this topic in the future.

ELICITING INFORMATION FROM DIGITAL TRACES

DAVID A. ELLIS[1] & LUKASZ PIWEK[2]

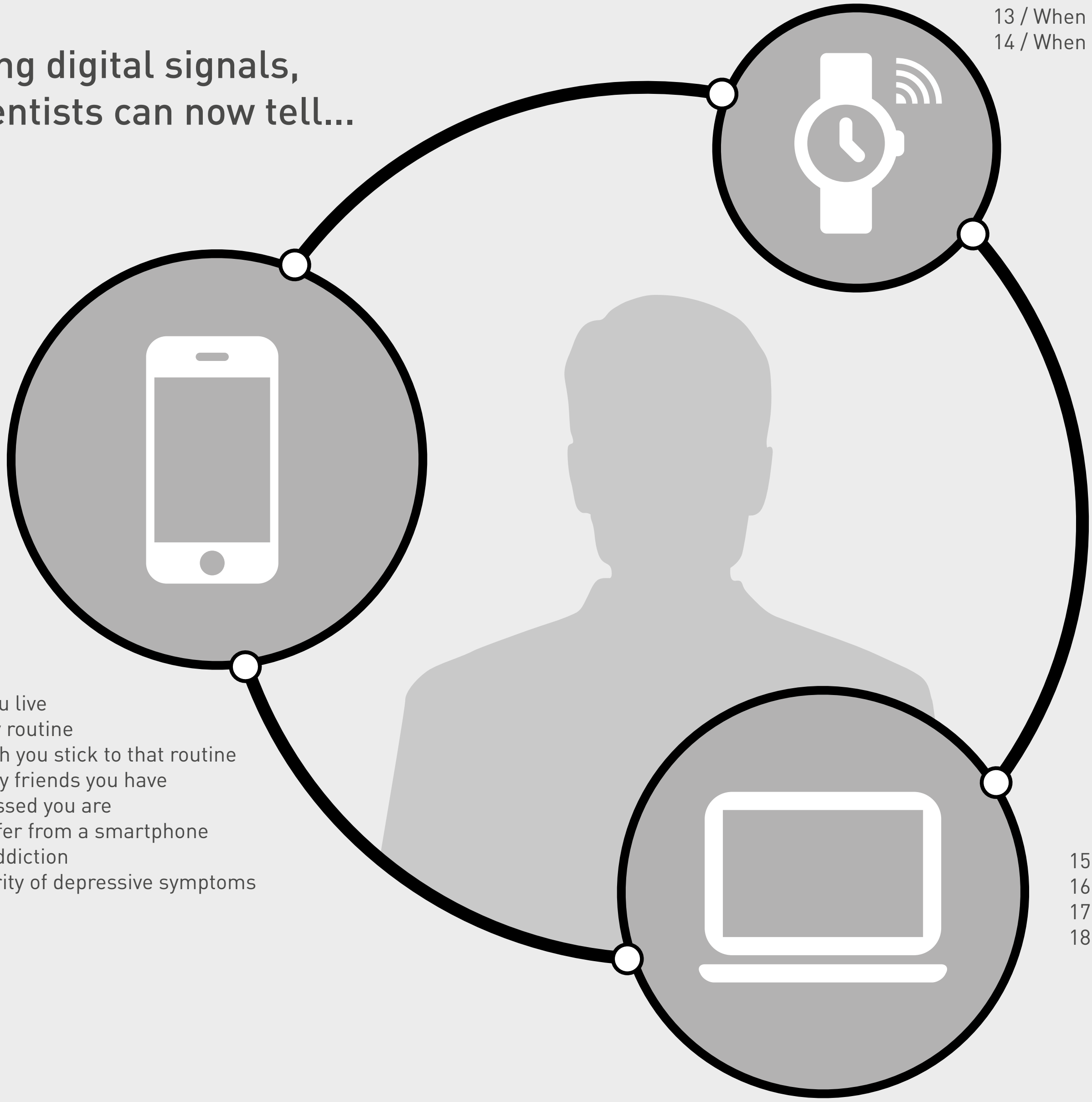
LIFE PATTERNS

On average, people check their smartphone 85 times a day. We also spend a significant amount of time interacting with other devices including tablets, laptops, and wearables. Our interactions with these can easily be recorded to better understand routine patterns of everyday behaviour. For example, because people spend most of their life in the same places, it is possible to predict where people are likely to go next based on GPS data from their smartphone. Similarly, an accelerometer placed on the wrist can, over time, build up a remarkably accurate picture of how well you are sleeping.

PERSONALITY

The distinctive words used within emails and social media allow for the accurate prediction of both complex (e.g. conscientiousness) and simple (e.g. age and gender) individual differences. Research has focused on traces of text left behind from social media and email, but call records and the type of applications used on each smartphone have been shown to predict a variety of personal attributes.

Using digital signals, scientists can now tell...



1 / Where you live
2 / Your daily routine
3 / How much you stick to that routine
4 / How many friends you have
5 / How stressed you are
6 / If you suffer from a smartphone related addiction
7 / The severity of depressive symptoms

8 / How well you sleep
9 / How fit/lazy you are
10 / Your mood
11 / When you get bored
12 / How fertility changes over a month
13 / When you are lying
14 / When you suspect someone else is lying

15 / Your personality as a whole
16 / How conscientious you are via emails
17 / Your gender and political views
18 / If you have psychopathic tendencies

EMOTIONS

Mood can be determined from text messages, but also from physiological data recorded by wearable devices. Increased heart rate and levels of sweat emitted from the body can indicate greater levels of physical activity, but the absence of movement may suggest increased levels of stress. Small samples of vocal information can also provide clues to an individual's current mood based on speech variability. Devices can accurately discriminate worry from confidence.

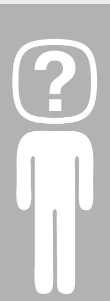
SOCIAL INFLUENCE

Combining digital traces from multiple people can be particularly revealing. The extent to which one person causes another person's behaviour provides a measure of influence, which can indicate a person's position in a social network and who they like and dislike. Tracked over time such measures give insights into team cohesion.

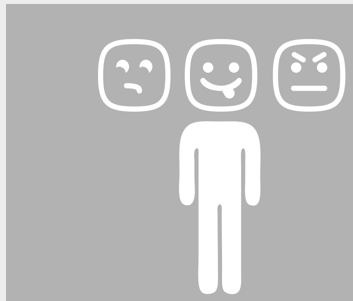
[1] Lancaster University, Department of Psychology &
[2] University of Bath, School of Management

WHAT YOUR PHONE SAYS ABOUT YOU?

LUKASZ PIWEK & ADAM JOINSON | UNIVERSITY OF BATH

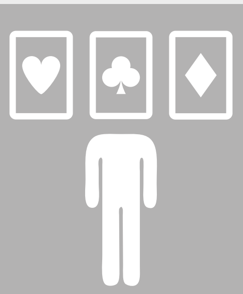


Your identity, with only few GPS location points [1]

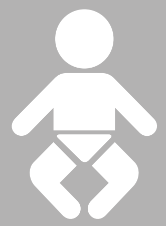


Your mood, using data such as length of your SMS & how fast you type or erase it [2]

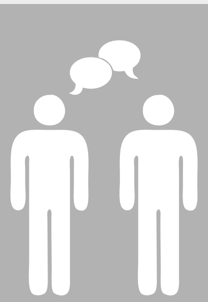
If you are stressed, based on call logs, SMS logs, and Bluetooth proximity data [3]



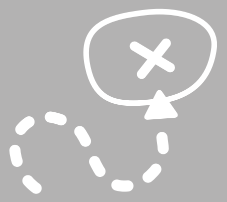
Your personality, using broad range of metadata like number of calls and SMS [4,5]



If you're a parent, based on apps usage patterns [6]

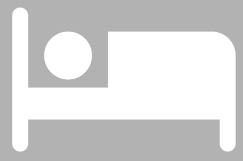


If you have a real-world chat with others using Bluetooth proximity [7]



Where are you likely to go next by analysing GPS data [8,9]

If you're sitting, walking, or running, by using accelerometer sensor [10,11]

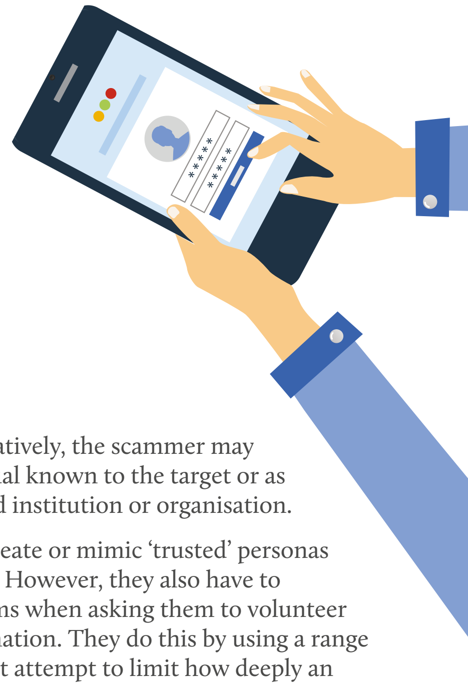


The quality of your sleep, also with accelerometer and only if you sleep with your phone [12]

[1] de Montjoye, Y.A., et al. (2013). *Scientific reports,* 3, 1376; [2] Lee & Park(2012). *Proceedings of IEEE CCNC,* 260–264; [3] Bogomolov, A., et al. (2014). *Proceedings of the ACM,* 477–486; [4] Chittaranjan, G., et al. (2013). *Personal and Ubiquitous Computing,* 17, 433–450; [5] de Montjoye, et al. (2013b). *Behavioral-Cultural Modeling and Prediction,* 48–55; [6] Seneviratne, S., et al. (2014). *ACM SIGMOBILE Mobile Computing and Communications Review,* 18, 1–8; [7] Osmani, V., et al. (2014). *Journal of Ambient Intelligence and Humanized Computing,* 5, 297–306; [8] Song, C., et al. (2010). *Science*, 327, 1018– 1021; [9] Do, T.M.T. & Gatica-Perez, D. (2014). *Pervasive and Mobile Computing,* 12, 79–91; [10] Wu, W., et al (2012). *Journal of Medical Internet Research,* 14, e130; [11] He, Y. & Li, Y. (2013). *International Journal of Distributed Sensor Networks,* 2013, 1–10; [12] Natale, V., et al. (2012). *Sleep and Biological Rhythms,* 10, 287–292.

EMMA WILLIAMS AND ADAM JOINSON

Eliciting Information Online



In November 2015, the Metropolitan Police Service reported that they had investigated £4m lost through internet dating scams in the previous 12 months. Given the likely under-reporting of losses by victims, it is probable that this figure represents a small portion of the total amount lost by UK internet users. In fact, in 2012 it was suggested that almost a quarter of a million people in the UK may have fallen for an online dating scam, a figure likely to have increased given the growth in online dating during the last four years. Online dating and romance scams work in part because relationships formed over the internet are vulnerable to 'hyperpersonal' patterns of interaction characterised by intense, accelerated feelings of closeness, rapport and trust. Because of this, the internet often provides an ideal environment for those with malevolent intent to elicit information from victims (see Box).

Causes of hyperpersonal interaction

There are a number of reasons why people often form overly positive, trusting relationships online that make elicitation of information more likely. These include:

Selective self-presentation: people choose what to communicate about themselves online – and usually that will be more positive aspects of themselves.

Idealised impressions: the person on the receiving end of these positive self-presentations often forms an idealised impression, with fantasy and social projection filling in the gaps.

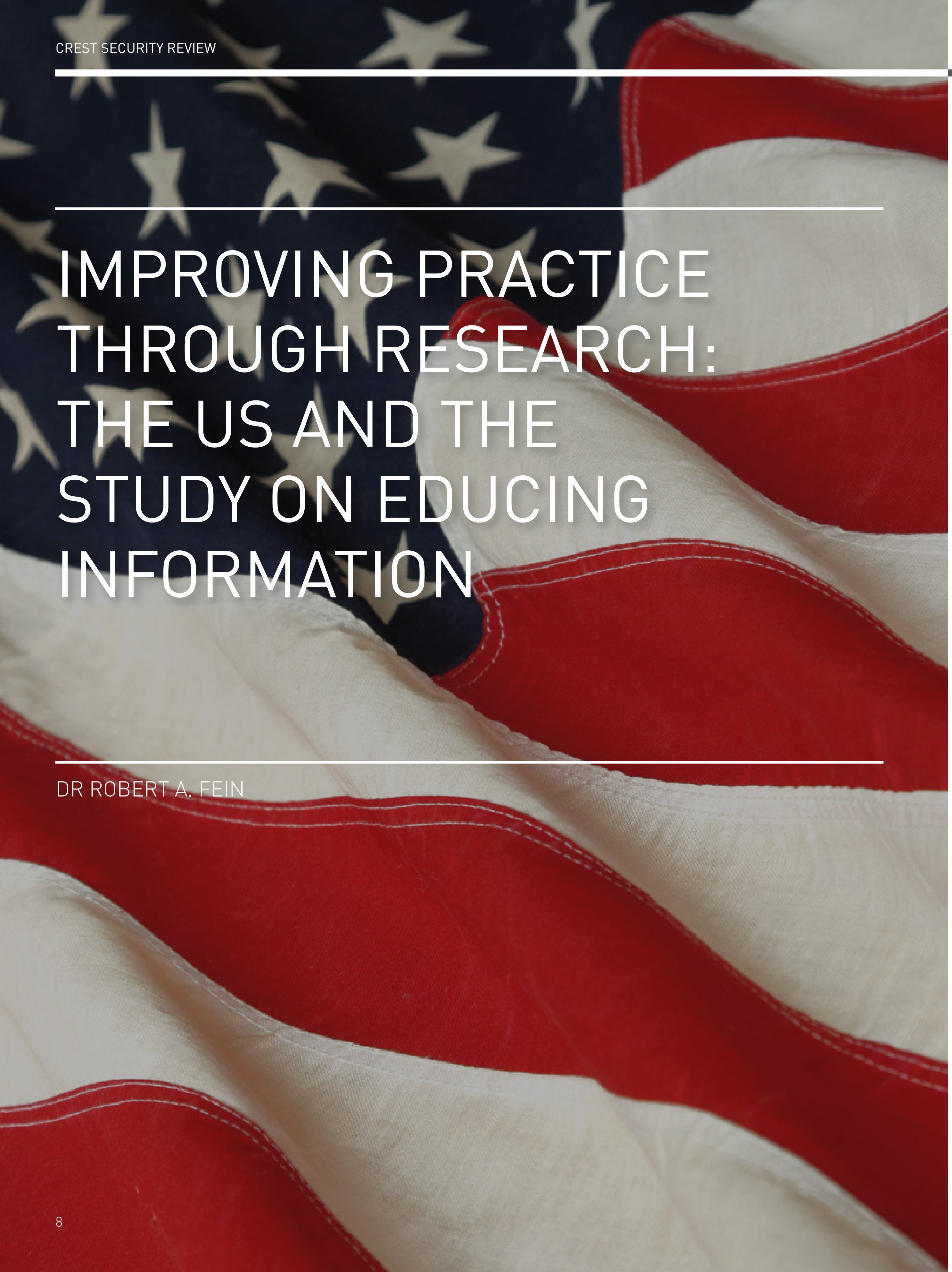
Confirmation biases: Once we form a positive impression of someone, we often seek information to confirm the initial positive impression, leading to a feedback cycle of positive impressions and increased liking.

Uncertainty reduction: People tend to disclose more information about themselves online – one reason being that uncertainty makes us uncomfortable. We tackle this uncertainty by asking more probing questions. We also tend to disclose more information about ourselves, which encourages the other person to reciprocate.

The nature of online communication means that scammers are able to strategically present and edit information about themselves, presenting profiles that appear similar (through apparent shared common interests or group membership) or attractive to the victim. For instance, online romance scams mimic coveted gender stereotypes in their profiles, such as wealthy widowers, military personnel, and young females in caring roles like nursing. Fake social media profiles have been used to infiltrate online networks of military and defence personnel, with such attempts being successful despite the presence of inconsistencies in profile information. Alternatively, the scammer may pose as an existing individual known to the target or as a representative of a trusted institution or organisation.

Online scams attempt to create or mimic 'trusted' personas in order to appear genuine. However, they also have to address the doubts of victims when asking them to volunteer potentially sensitive information. They do this by using a range of influence techniques that attempt to limit how deeply an individual processes information, encouraging them to make relatively automatic decisions based on stereotypes and biases. This includes creating scenarios that invoke a sense of urgency so that victims feel they don't have sufficient time to verify them, or creating an imminent crisis and asking for help so that people feel obliged to respond, particularly if emotions such as empathy, guilt or anxiety are invoked. For this to work they have to generate an emotional response from the victim through helping them identify with the character and situation they are presenting. Techniques designed to create an obligation of reciprocity in the future may also be used, such as providing free gifts or favours and requesting information in return. This combination of 'editable' online personas and complex influence scenarios may make people particularly vulnerable to information elicitation attempts in online environments.

Emma Williams and Adam Joinson research scamming techniques and are based at the University of Bath.



IMPROVING PRACTICE THROUGH RESEARCH: THE US AND THE STUDY ON EDUCING INFORMATION

DR ROBERT A. FEIN

National Security psychologist Dr Robert A. Fein was a member of the US Intelligence Science Board and Chair of its Study on Educing Information from 2004-2009. Here he writes about how this study helped the United States learn from the latest research on eliciting information and improve their knowledge and practice.

In the months and years following the attacks on the United States on September 11, 2001, the US government captured and detained many people it believed had ties to al-Qaeda or related terrorist organisations. Interrogating these detainees was seen as an important way to get information that might help prevent future attacks. However, the US government had little experience conducting interrogations since World War Two.

Responding to a knowledge gap about interrogation, in 2004 the Intelligence Science Board (ISB), a group set up by and for the US Intelligence Community to provide it with expert advice, was asked to conduct a study examining what was known from science about interrogation. This effort, the ISB Study on Educing Information, was designed to be an engine of change study. We had two central goals: to review the science relevant to interrogation, and to engage government experts and organisations in efforts to improve knowledge and practice.

Throughout the study, we worked hard to maintain the trust of the professionals and organisations we worked with.

In the first phase of the project, we reviewed the history and current practice of interrogation and interviewing in the US and beyond, and engaged with practitioners and policy-makers.

In the second phase, we visited the United Kingdom, France, and Japan, worked with a team of intelligence and behavioural science experts, and developed an evidence-based "intelligence interviewing" framework. The framework included factors that the scientific evidence shows are relevant to effective interviewing, including stress, the interests and social identities of interviewees, sources of power in interviewing, interviewee resistance, persuasion, changing perceptions, and memory, as well as two teaching case studies.

Throughout the study, we worked hard to maintain the trust of the professionals and organisations we worked with. We stayed out of the media, sought guidance and perspectives from senior intelligence community leaders, and provided regular briefings to the Intelligence Science Board and members of sponsoring organisations. The Study on Educing Information concluded in 2009.

Seven years later, how do I see what we accomplished?

First, we encouraged and facilitated knowledge-based discussions of a politically charged topic. We brought together professionals from a range of disciplines and organisations to share experiences and expertise, hoping to bring light to heated debates. We provided materials and briefings that encouraged national security leaders to move forward, in this small, but significant, area of human intelligence collection.

Second, we highlighted the importance of knowledge-based efforts in intelligence interviewing and interrogation. We recommended further research. We contributed to the US Government developing the High Value Interrogation Group (HIG) and, importantly, providing the HIG with resources for a robust research program.

The US government had little experience conducting interrogations since World War Two.

And third, as we have seen in presentations to intelligence professionals—that were based on the intelligence interviewing framework and the case studies we developed—we were able in a small way to help bridge the gap between knowledge and practice. Developing operationally useful knowledge and communicating that knowledge to professionals who need it and can use it remain major challenges in US, and in other, national security communities. These challenges are met through initiatives such as the US's Educing Information Study and the UK's Centre for Research and Evidence on Security Threats.

WANT TO READ MORE?

Phase 1 report of the Educing Information study – a primer on the science of interviewing.

Teaching papers and case studies from the Educing Information study: https://fas.org/irp/dni/isb/interview.pdf

In the next issue we'll discuss the legacy of the Study on Educing Information through the High value Interrogation Group. In particular we'll examine how it has helped to challenge coercive and ineffective interview practices and put evidence-based techniques at the heart of training and practice in the US and beyond.

THE A TO Z OF INFORMATION ELICITATION

A is for active listening, a technique that involves using a paraphrased summary of what the other person has said in order to show a willingness to listen, and give them the opportunity to correct any errors.

B is for baselining, and evidence showing that prior exposure to a person tends to facilitate our ability to identify truth-telling in a future encounter, but not necessarily our ability to identify deception.

C is for cognitive interview, an approach that encourages detailed, open-ended reporting and uses techniques that aid memory recall: by almost 80%. See the CREST website for our guide to the cognitive interview.

D is for decay, and the finding that information campaigns to counter telephone based social engineering attacks work after one week, but are useless after two weeks.

E is for educing, a word the US National Science Foundation chose over elicitation in their must-read and still very relevant 2006 report 'Educing information.' See page 8.

F is for flattery, and the fact that even blatantly insincere flattery — the kind spotted by its target — has been shown to improve cooperation and liking. You gorgeous reader, you.

G is for grouping, and the advantage that comes from interacting with two people simultaneously. They typically provide more detail (e.g., as they correct one another) and give away their deception more readily.

H is for heuristic, and research showing that we use proxies such as 'what others are doing' to determine our willingness to comply to requests.

I is for interpreter, whose demeanour, approach to translation, and even seating position has been shown to impact the amount of information a person reveals.

J is for judgement error – and the discovery that making an incorrect inference about a person's state of mind or motivation will reduce trust and cooperation, but also lead to greater information provision. Use sparingly!

K is for kindness, an approach that can backfire when used with high context cultures (e.g., Chinese, Russian) who can interpret it as patronizing and questioning their capacity.

L is for language and evidence showing that adopting the same words as another is enough to make them cooperate and like you more. It also predicts relationship stability.

M is for motivational frame, and evidence that shows people tend to frame issues through an identity, relational, or instrumental lens. Adopting the same frame is critical to cooperation.

N is for nonverbal behaviour, and evidence showing that a message accompanied by a nonverbal style that matches the preferred style of the recipient is more likely to be received positively and lead the recipient to desire to act as requested.

O is for open questions, the cornerstone of getting good information. Sir William Osler's 1898 dictum to medical students – "Listen to the patient, he is telling you the diagnosis" undoubtedly applies to security settings too.

P is for phishing, and evidence showing that we're more likely to click at certain times of day, such as just before lunch.

Q is for quality, as a reminder of the ever-present danger of mistaking quantity of information elicited with its quality. The former is useless if it is low in quality.

R is for rapport, and evidence showing that alleged terrorists in police interviews respond to interviewers who demonstrate empathy and acceptance, and who allow the interviewee autonomy in their account.

S is for strategic use of evidence, and data showing that withholding evidence until after you've asked specific questions about it provides a useful tool for detecting deception as liars have to continuously change their story.

T is for timeline technique, a structured debriefing method from Lorraine Hope that has been shown to increase the amount and detail of information about who did what, when, and with whom. See the CREST website for a guide to the Timeline Technique.

U is for undergraduates, which is still the group studied in most research on information elicitation. This is unfortunate, as recent research suggests common techniques do not work as well with interviewees of different ages and cultures.

V is for volunteering information, often known as self-disclosure, which when used carefully can encourage the disclosure of information in others.

W is for window, which is one thing that work on 'priming' shows can encourage disclosure when left open. The work shows that our behaviour is moderated by the context in which we find ourselves, so lots of cues to openness encourages cooperation.

X is for XSens, a technology that enables full-body motion tracking that has been used to allow investigators to watch back their behaviour when eliciting information from others. It has also proven more effective than the polygraph at identifying liars.

Y is for 'yes,' 'uh-huh,' 'ok', and all the other positive backfeeds that have been shown to encourage people to keep talking (and in so doing provide more information).

Z is for Zelig, a statistical measure of the degree to which a person is an interpersonal chameleon; the extent to which they adapt their behaviour to match the person with whom they interact. High Zeligs are more likable and often elicit cooperation as a result.

PAUL TAYLOR

The promise of social science

What can social science offer our understanding of security problems? CREST Director Paul Taylor outlines some of the successes and challenges.

From understanding what drives a terrorist to cataloguing the behaviours of a loyal employee, the security world is littered with 'human' problems. Yet not everybody is convinced that a 'science of us' is needed to solve such problems and such arguments are not without merit; what has social science given us beyond common sense?

That social science often feels like common sense stems from the fact that we all are, to some extent, social scientists. It is the science of our everyday experience. It dissects the things we know a thing or two about. Answering even a simple social science question can involve painstaking work, as anyone who's attempted ethnography or the tireless coding of case material will attest. But answers can confirm our preconceptions, and so are perceived as obvious. And when results don't conform to our intuitions? It's tempting to dismiss findings rather than embrace their novelty and change our worldview.

Many of the successes of social science are characterized by fights against intuition. It took several decades of evidence to dispel the widespread perception that terrorists were 'crazy' and somehow 'different in the head' to others. Now we understand such behaviour to be the result of social pressures and personal motivations, which are as idiosyncratic as the reasons people give for joining government and police organisations that tackle the threat. There are still those who seek a checklist, an 'extremism thermometer,' an automated online identifier, and other one-stop solutions that whittle the complexity of extremism down to a few variables and ignore the false positives. But at least the evidence has the upper hand in most circles.

That social science often feels like common sense stems from the fact that we all are, to some extent, social scientists.

Other fights still continue. One covered in this issue of *CSR*, which continues to beget conversations in North America and elsewhere, is the role of 'enhanced interrogation.' Despite evidence suggesting that the best way to elicit information is to build rapport and engage in good questioning, there are some who still see a place for torture. It took several decades of the last century for UK police interviewing practice to adopt the investigative interviewing model that is so engrained, and so effective, today. It will similarly take time for the evidence against coercive or harsh techniques to gain full acceptance. How much time depends on open-minded practitioners and policy makers being willing to weigh the evidence against their intuition.

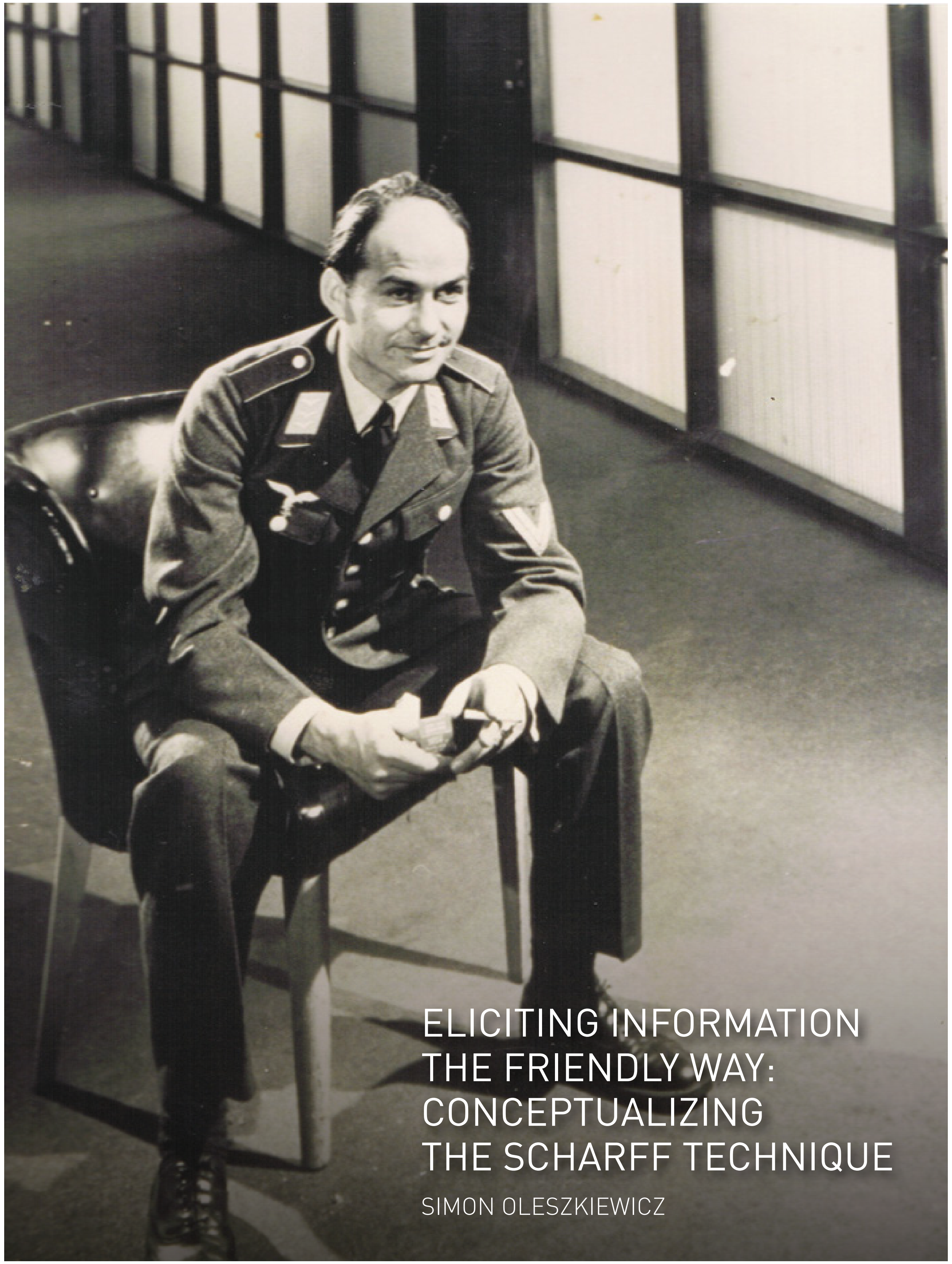
One promise of social science is developing methods that are grounded in rich empirical evidence. The investigative interview described on page 22 is an example of that. A second, recent example that is developing rapidly in the security field is at the interface of the digital and human. Behavioural and social scientists can access data in new ways thanks to technological advancements. Assessments of personality, interpersonal dynamics, and social moderators of behaviour have become measurable and testable.

On other occasions social science adds value not by discovering something new, but by packaging it up in a digestible way. A tool taught to crisis negotiators and interviewers across the world, known as the cylinder model, is a simple articulation of the different goals that speakers pursue when talking. At its heart is a distinction between speaking about a want or desire (e.g., "What is your name?"), speaking to manage affiliation and trust (e.g., "It's nice to see you"), and speaking to address identity ("Wow you look great"). A quick introspection will confirm that we do use language in these ways; so nothing new here. But the systematic representations of this in the cylinder model has proven useful for training, for planning difficult conversations, and for debriefing incidents once they have happened. If nothing else, the model gives everybody involved a common language for describing what has gone on.

Packaging common sense in a deliverable, repeatable, way – like the cylinder model; measuring and testing our common sense; dispelling myths and folk knowledge where necessary are all examples amongst many that the promise of social science is being delivered now. In the complex mix of human problems that are so central to questions of security – these gains, even if small, are essential.

You can read more about the cognitive interview, mentioned in this article, on the CREST website at www.crestresearch.ac.uk

It took several decades of evidence to dispel the widespread perception that terrorists were 'crazy' and somehow 'different in the head' to others.



ELICITING INFORMATION THE FRIENDLY WAY: CONCEPTUALIZING THE SCHARFF TECHNIQUE

SIMON OLESZKIEWICZ

"Did your plane carry bombs in it or didn't it? You cannot ask that direct question, he will never answer it. But in the course of a regular conversation he will probably drop somewhere an indication that he did or he didn't, without even knowing what he said."

These are the words of the renowned WWII Luftwaffe interrogator Hanns Scharff (1907-1992) explaining to the Pentagon how he extracted information from allied fighter pilots without alerting them of their contribution. Quotes like these may be thought provoking for most, and within the head of this experimental researcher it resulted in a large neon sign twinkling "components" surrounded by question marks. So then, what are the mechanisms that allow a person to systematically steer another to reveal information unknowingly? Through a 4-year long research program my collaborators and I have started to address that question.

So what made Scharff so effective? To answer this we first have to know what he did. We began by breaking down Scharff's approach into individual tactics.

Scharff's tactics were built on the understanding of the typical behaviors of sources. By putting himself in the shoes of an allied prisoner, Scharff identified at least three general behaviors that were used to avoid providing information that would advance the interviewer's knowledge: (1) I will not tell very much; (2) I'll try to figure out what they are after and not provide that information; (3) It is meaningless to deny/hold back what they already know.

Having identified some resistance strategies Scharff developed his own tactics to circumvent them. The first tactic was to maintain a friendly approach. Scharff avoided coercive methods and became known for his equality-oriented approach. The second tactic was not pressing for information. Rather than demanding answers to questions, Scharff would tell stories, related in such a fashion as to encourage conversation and leave openings for the source to fill in. The third tactic was to build an illusion of knowing it all. Scharff would often open the interview by telling a detailed story that demonstrated his knowledge, which made it clear that he already held a large amount of correct and detailed information. The fourth tactic was confirmation/disconfirmation. Instead of asking direct questions, Scharff presented claims that he wanted to have confirmed or disconfirmed by the prisoners. The fifth tactic was to ignore new information. When provided with critical information, Scharff would downplay it as unimportant or already known, hiding the fact that the information was of interest to him.

SCHARFF'S TACTICS WERE BUILT ON THE UNDERSTANDING OF THE TYPICAL BEHAVIOURS OF SOURCES.

In our laboratory we have conducted a series of experiments where we compared the Scharff technique, conceptualized as these five tactics, against asking a combination of open-ended and specific questions (i.e., the direct approach). The Scharff technique consistently resulted in more new information, as well as better masked information objectives, compared to asking explicit questions. Furthermore, the Scharff technique consistently influenced the sources to underestimate their contribution. In stark contrast, the sources in the control condition tended to overestimate their contribution.

So what makes the Scharff technique more successful than posing explicit questions?

Sources who adopt resistance strategies are likely to try to estimate what information the interviewer already knows and what information he or she is after. Such assessments will inform on what information to reveal and what to withhold. Our studies show that when these sources are approached with explicit questions they will believe the interviewer knows very little about the topic under discussion. In such cases sources will perceive that almost everything they reveal will advance the interviewer's knowledge.

In direct contrast, the aim of the Scharff technique is to influence the sources to perceive the interviewer as knowledgeable. Consider an interviewer who starts the interview by presenting all information already held on the case. If the source then wants to be perceived as cooperative, she cannot simply repeat the information already stated by the interviewer. Instead, the source will need to go beyond the interviewer's story and provide new information. Hence, for information gathering purposes, the known information can be presented at the outset of the interview in order to direct the source away from already known information and towards new information.

In conclusion, the Scharff technique is designed to increase the outcome for the interviewer when sources are not completely cooperative. During such circumstances the interviewer can use already known information to steer sources towards previously unknown information and lead them to unknowingly increase the value of their contribution. Hence, science does not only support the wisdom of a master interrogator, it helps to clarify general components that go beyond individual talents.

WANT TO READ MORE ABOUT THE SCHARFF TECHNIQUE?

Download the author's dissertation at the following link: https://gupea.ub.gu.se/handle/2077/41567

Simon Oleszkiewicz works in the Department of Psychology at the University of Gothenberg. His research into the Scharff technique was funded via the FBI's High-Value Detainee Interrogation Group.

How does memory work?

LORRAINE HOPE

Interviewing survivors of, witnesses to, and participants in terror attacks enables investigators to piece together what happened and how. Understanding how the memory works can help interviewers obtain more information with greater accuracy. In this feature Professor Lorraine Hope gives us an important insight to what interviewers need to know.

It is perhaps easier to describe how memory doesn't work. It doesn't work like a video-recorder. It doesn't work like a hard-drive of a computer. And it definitely doesn't work like a library filled with shelves securely storing pristine copies of our experiences. Instead, our memories are mental constructions and re-constructions of experienced past events. As a result, although often reliable, our memories are also fallible. At best, our initial recollections may be incomplete or lacking in detail. At worst, they may be distorted, contaminated or just plain wrong.

For anyone faced with the task of obtaining accurate and detailed information from another person, whether in a formal interview, an informal interaction or other law enforcement or intelligence gathering contexts, understanding a few key features of memory is critical.

MEMORY IS TRANSIENT

Memory fades over time. We lose access to details and specific information. Put plainly, we forget. After a delay, we might only remember the gist of an experience, a witnessed event or a conversation. Typically, forgetting occurs quite rapidly, making it important to attempt to obtain information about a particular incident or experience as soon as possible.

MEMORY IS SUGGESTIBLE

Our memories for events are easily distorted by information encountered after the event took place. Distortions can range from relatively minor errors (such as a small mistaken detail) through to entirely false memories for events that never took place. Interviewers often inadvertently contaminate memory by asking (mis)leading questions that suggest particular details to the interviewee. An easy way to avoid contaminating memory is to use open-ended questionsto encourage the interviewee to report information in their own words – based on their own memories. Why ask "Was the man wearing a black coat?" when you can ask "What was the man wearing?"

MEMORY IS SOCIAL

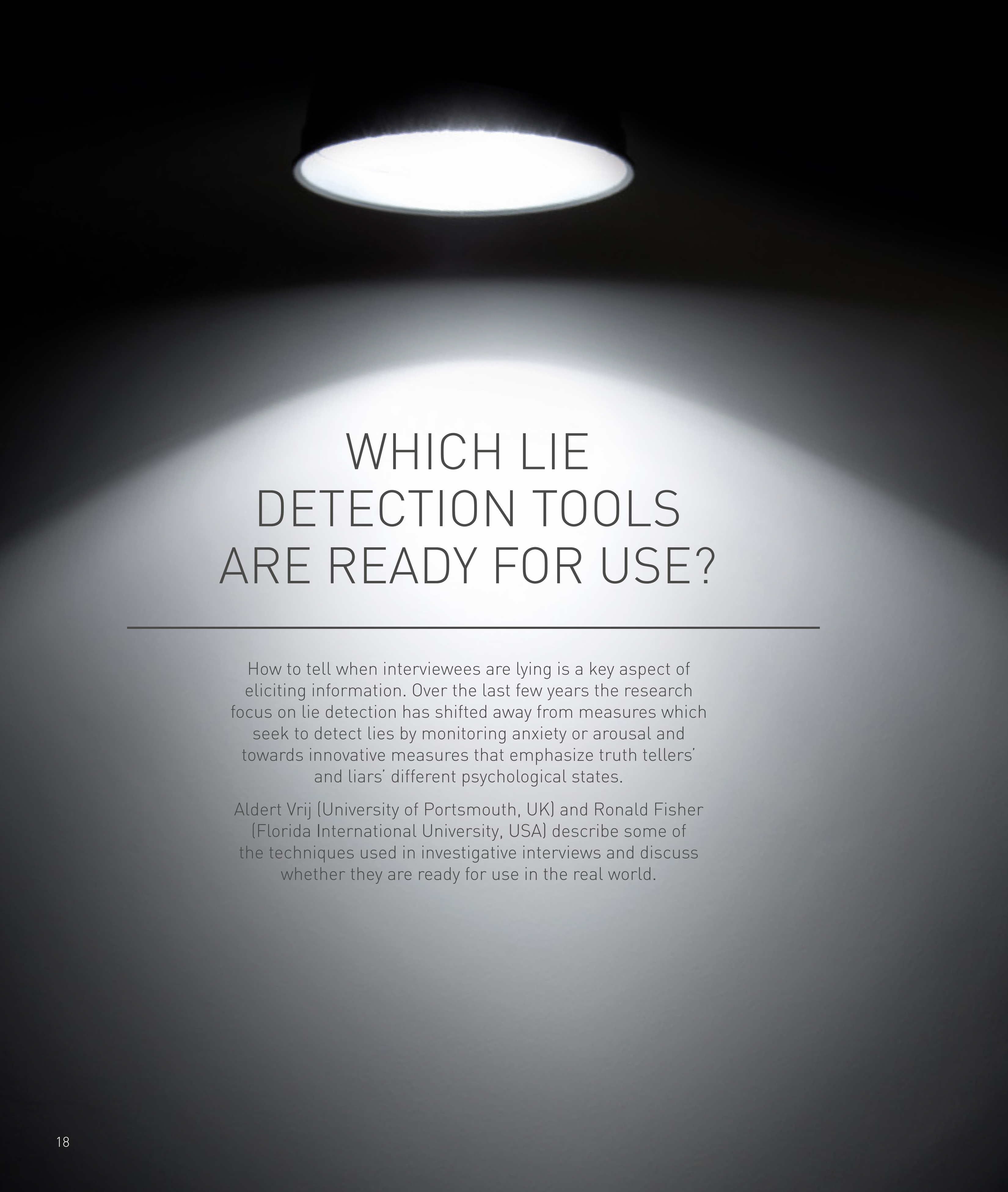
Memory serves a social function - we share our experiences with others to inform, to build bridges, to entertain. In this way, conversations with others can change the way we remember events. The way in which this 'social contagion' occurs means that we may not detect a discrepancy between our now contaminated memory and our original experience. So it's important for an interviewer to determine whether the events reported were experienced first hand or reflect a second hand tale. This can be particularly important in cultures where collective experience is highly valued. It is also worth determining whether the experience has been discussed with others who may have been present. Finally, if eliciting information from several individuals who have discussed an incident with each other, bear in mind that consensus may not reflect an accurate account but rather cross-contamination of individual memories within a group.

MEMORY NEEDS HELP

Remembering can be a demanding mental task. It requires effort and motivation on behalf of the person doing the remembering. A good interviewer can help support the recollection process in a number of ways. Allow the interviewee to relax and take time to mentally revisit the original experience, for instance, and use open questions that prompt for further information without suggesting misleading information. Interviewers can also promote recall in different formats, including through the use of sketches or timelines and by avoiding pressurising closed questioning and interruptions. But remember, some interviewees may be over-keen to please or more motivated by reward than accuracy – both of which may result in the reporting of erroneous information. Always explicitly give interviewees an opportunity to say they don't know or simply can't remember any more information.

Memory is an important source of investigative and security-critical information. As with any source, the careful handling of memory can offset many of the vulnerabilities inherent in the recollection of our past experiences.

Lorraine Hope is Professor of Applied Cognitive Psychology at the University of Portsmouth. She is an expert on the role of interviewing and function of memory in investigatory settings. You can read her introductory guide to using the Timeline Approach in interviewing on the CREST website.



WHICH LIE DETECTION TOOLS ARE READY FOR USE?

How to tell when interviewees are lying is a key aspect of eliciting information. Over the last few years the research focus on lie detection has shifted away from measures which seek to detect lies by monitoring anxiety or arousal and towards innovative measures that emphasize truth tellers' and liars' different psychological states.

Aldert Vrij (University of Portsmouth, UK) and Ronald Fisher (Florida International University, USA) describe some of the techniques used in investigative interviews and discuss whether they are ready for use in the real world.

AROUSAL-BASED LIE DETECTION TOOLS

Behaviour Analysis Interview (BAI). The BAI consists of a set of standardized questions. It is assumed that during the BAI liars feel more uncomfortable than truth tellers and display more nervous behaviours (e.g., crossing legs, shifting about in chairs, performing grooming behaviours, or looking away from the investigator).

Comparison Question Test (CQT). During a CQT examinees are attached to a polygraph machine and are asked relevant questions, e.g., 'Did you murder Joe Frisbie on March 12, 2016'? and comparison questions, e.g., 'Before 2015, did you ever physically injure someone who loved and trusted you?' The theory behind CQT suggests that innocent suspects will become more concerned with the comparison questions than with the relevant questions. Examinees who react most strongly to the comparison questions are considered truthful and examinees who react most strongly to the relevant questions are considered deceptive.

COGNITIVE-BASED LIE DETECTION TOOLS

Imposing Cognitive Load. Lying is in interview settings typically more mentally taxing than truth telling. Investigators can exploit this by making the interview setting cognitively more difficult, for example by asking interviewees to engage in a concurrent, second, task when discussing the event. Liars, whose mental resources are more depleted, are less able than truth tellers to cope with additional requests.

Asking Unexpected Questions. When investigators ask a mixture of anticipated and unanticipated questions, truth tellers answer these questions with similar ease, but liars find answering the unanticipated question more difficult than answering the anticipated questions.

Encouraging Interviewees to Say More. When encouraged to add to their original account, liars provide less new information than truth tellers. They do this because they find it cognitively too difficult to add many plausible sounding details or may be reluctant to add more details out of fear that it will provide leads to investigators which can give their lies away.

Strategic Use of Evidence (SUE). During interviews truth tellers are generally forthcoming, whereas liars are more inclined to avoid mentioning where they were at a certain time, or use denials (e.g., denying having been at a certain place at a certain time when asked directly). When investigators ask questions related to the evidence without making the interviewee aware that they possess this evidence, these different behaviours used by truth tellers and liars result in truthful suspects' accounts being more consistent with the available evidence than deceptive suspects' accounts.

Verifiability Approach (VA). Liars are aware that accounts rich in detail are more likely to be believed, but also fear that investigators will check such details. Their way around this problem is to provide details that cannot be verified. Liars use this strategy and typically report fewer details that can be checked than truth tellers.

Concealed Information Test (CIT). A CIT polygraph test can be used when examinees deny knowledge of a specific crime. During the test examinees are given questions with multiple-choice answers (e.g., "How did the murderer kill his victim: Did he i) drown her; ii) strangle her with a rope; iii) stab her with a knife or iv) shoot her with a gun?") A deceptive examinee will recognize the correct answer which produces a (physiological) orienting response. A truthful suspect does not recognize the correct answer and will not show an orienting response.

WHICH LIE DETECTION TOOLS ARE READY FOR REAL-WORLD USE?

There is substantial difference in the extent to which the eight lie detection techniques could be said to be ready for real world use in investigative interviews. The two arousal-based techniques fall short on numerous criteria although they are currently used frequently. For example, they are prone to false-positive errors as truth tellers can easily appear nervous or anxious during tests. There is not enough evidence for reliable error-rates for the BAI, and both the BAI and CQT require substantial training and cannot be used as part of standard interviews – making them harder to utilise.

Of the cognitive approaches, there are too many problems associated with the imposing cognitive load technique to recommend it for use in real life, but other techniques are ready for use ('Encouraging Interviewees to Say More' and SUE) or ready for use if they continue to receive support in empirical research ('Asking Unexpected Questions' and VA). The CIT polygraph test cannot be included in a standard investigative interview. It can be a useful tool in addition to investigative interviewing although it has been criticised because it cannot be used in many situations (for example, it can't be used when the interviewee partially accepts knowledge of the crime).

This article is based on a forthcoming article in the Journal of Applied Research in Memory and Cognition (JARMAC). This includes a comparison of each approach against ten criteria including five derived from US Criminal System guidelines.

WHAT'S THE DIFFERENCE BETWEEN SUNNI AND SHIʿA MUSLIMS?

Understanding the differences between the two most populous branches of Islam is essential for comprehending many of the geo-political conflicts in the Middle East as well as community tensions in diasporic communities in the West. Kim Knott and Matthew Francis put a few of the key issues in context.

The vicious and devastating cycle of violence in Iraq between Sunni and Shiʿa groups is an all too frequent reminder of the dangers of sectarian conflict. With that in mind it is perhaps not surprising that the differences between these communities are frequently blamed for tension between Muslims not just in the Middle East but elsewhere too. However, Sunni and Shiʿa communities have a lot more in common in their beliefs and practices than they have differences. In fact in countries where populations and access to power are relatively equal they have tended to live together peacefully. Generally where conflict has arisen this has been due to power imbalance or geo-political conflict (such as between Iran and Saudi Arabia) than ideological difference. Indeed in some countries sectarian conflict is more likely to occur between different Sunni groups than between Sunni and Shiʿa communities.

Shiʿas make up about 10% (approximately 162 million) of the global Muslim population and form a majority in five countries: Azerbaijan, Bahrain, Lebanon, Iran and Iraq.

Image credit: Mirror writing depicting the Shia "Ali is the vicegerent of God". The original panel is in the Library of Congress.

SIMILARITIES

The following central Islamic beliefs and practices are shared by both communities:

– **Qur'an** – All Shiʿa and Sunni Muslims accept the centrality of the Qur'an – there is no truth to the accusations that Shiʿa use a corrupted version of the text.

– **Hadith** – Shiʿa and Sunni Muslims both draw on the Hadith – although tend to favour different collections of sayings.

– **Five Pillars of Islam** – Both groups also accept the five pillars of Islam (Shahada, the declaration that "There is no God but God, and Muhammad is His messenger."; Salah, prayer; Zakat, charitable giving; Sawm, fasting in the month of Ramadan; Hajj, pilgrimage to Mecca.)

Shi'ism should not be thought of as a later offshoot of Sunni Islam – the two only assumed their current forms in the ninth century CE, after the end of the line of Shiʿa Imams and the collection of the Prophet's sayings (Hadith) had been finalised. Both are considered orthodox and Al-Azhar University in Cairo (the world's oldest Muslim university and a Sunni institution) recognises both in its curriculum. In many parts of the world Sunni and Shiʿa have lived together peacefully and even intermarried.

DIFFERENCES

The primary ideological difference relates to questions of religious authority and the leadership of all Muslims following the death of the Prophet. Those who followed the Prophet's closest companion (Abu Bakr) became known as Sunni (the followers of the Prophet's example – Sunnah). Those who followed the Prophet's cousin and son-in-law ('Ali) became known as Shiʿa (the followers of the Party of 'Ali – Shiʿatu Ali). Sunnis focus on following the Prophet's example whereas Shiʿa focus on the lineage of Muhammad's family through a series of Imams.

Since the 1970s, and especially since the Iranian Revolution in 1979, there has been growing tension between Sunni and Shiʿa communities in parts of the Middle East. The Iranian Revolution led to the rise of a Shiʿa theocracy which has since supported Shiʿas in Iraq, Saudi Arabia and Bahrain as well as supporting Hezbollah (Lebanon), Hamas (Gaza), and the Syrian regime of Bashar al-Assad. Shiʿa dominated governments in Iraq and Syria have committed violence against Sunni populations. Likewise, the foundational alliance between Wahhabism and the rulers of Saudi Arabia has seen Shiʿa movements marginalised there and Shiʿa communities in Iraq have been subjected to extreme violence at the hands of the Sunni ISIS.

Sunnis focus on following the Prophet's example whereas Shiʿa focus on the lineage of Muhammad's family through a series of Imams.

Further afield, tensions between Sunni and Shiʿa communities are reported to be on the increase in diasporic communities in the West. In 2013 one demonstration led by the Sunni preacher Anjem Choudary in the UK included banners which proclaimed that Shiʿa were the enemies of Allah. Sectarian violence in Iraq and Syria have fuelled tensions in the UK, with divisions hardening in places like student societies. However, it is worth noting that Wahhabist influence has also led to hardened divisions within Sunni Islam too.

A version of this article appeared on the CREST website. Based on work by Kim Knott CREST has produced a guide to improve understanding on this subject: 'Sunni-Shiʿa Islam: Differences and Relationships'. Visit the CREST website to read the guide.

JORDAN NUNAN & REBECCA MILNE

Turning research into practice in investigative interviewing

Over the past thirty years researchers united with practitioners have confronted real-world investigative problems with science and have come to together to create solutions. This is particularly salient in the case of investigative interviewing, where research has helped bring about a transformation in how police in the UK understand and use interviews.

The purpose of the majority of investigative interviews is to elicit the most detailed, accurate, and complete accounts from the interviewee. With that in mind, being able to establish what happened and who did what is a vital skill and this derives from following effective interviewing practice. Detailed and reliable information is so important to investigations because it helps inform investigative decisions: the better the information, the better the decisions. However, it is important that information should not be obtained 'at any cost'. Interviewing needs to be ethically conducted in order to obtain information that is legally, and indeed factually, reliable. As research has shown, the history of police interviewing in England and Wales has seen the consequences of unethical and ineffective practice and the resultant unreliable evidence that follows from these practices.

HOW RESEARCH CHANGED INTERVIEWING

The concept of a successful interview has changed hugely since the 1970s. Prior to the early 1990s, no formal interview training was provided to police officers across England and Wales, as back then trainees were expected to learn by observing experienced colleagues. Often these experienced colleagues promoted methods which were purely focused on getting a confession, as gaining a confession was perceived to be a successful interview.

However, methods like these contributed to cases such as the Guildford Four (1975) and Birmingham Six (1976) which are prime illustrations of how unethical interviewing can lead to miscarriages of justice. The public outcry which followed the overturning of those verdicts led to the integrity of police interviewing practices being questioned.

Interviewing needs to be ethically conducted in order to obtain information that is legally, and indeed factually, reliable.

Police interview practice has developed over time, hand in hand with research. A milestone was the 1984 Police and Criminal Evidence Act, which mandated the recording of suspect interviews. For the first time, researchers were able to conduct an in-depth analysis of police interviews with suspects, published by the UK Home Office in 1992. This highlighted serious shortcomings, including lack of preparation, poor technique and assumption of guilt, in more than a third of police interviews. The report led directly to the development of a UK national framework of interviewing (PEACE).

The PEACE framework outlines the phases of the interview:

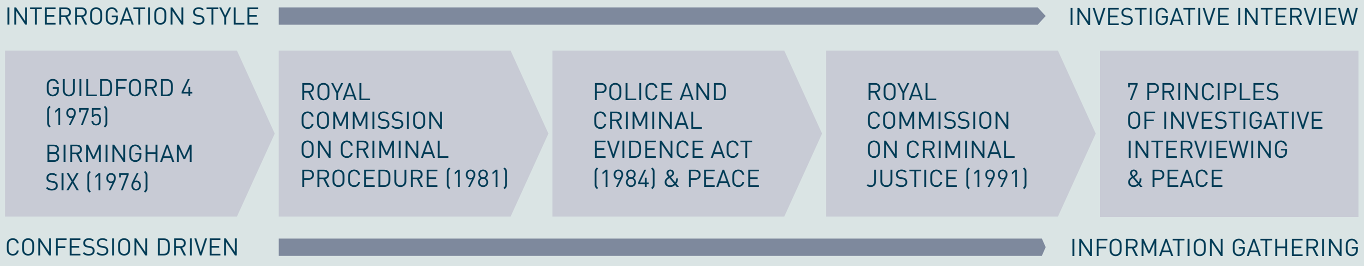
- **Planning and preparation** – where to hold the interview, what is known about the interviewee and what needs to be proved?
- **Engage and explain** – explain what the interview is for, engage the interviewee in a conversation
- **Account, clarification and challenge** – use open questions, allow interviewee to explain their account
- **Closing down the interview** – summarise the account given and explain what happens next
- **Evaluation** – evaluating the information received, the interview process itself and the performance of the interviewers.

While the general focus of investigative interviewing has improved since the introduction of PEACE, this impact appears to be primarily concerned with the more procedural and legal aspects of the interview rather than the more complex interviewing skills required. Aspects of investigative interviewing remain demanding for interviewers, such as how to challenge accounts in a non-confrontational but useful way, and these skills need to be maintained through repeated training.

WHERE RESEARCH IS HELPING NOW

Research continues to analyse and improve interviewing techniques. This includes work on the role of interpreters, on how cultural differences can affect the information offered by interviewees, and new techniques for uncovering deception. While these may not have such a seismic impact as the improvements in UK police interviewing approaches in the last thirty years, there is no doubt that the continued interaction of researchers and interviewing professionals is a positive and productive partnership.

Read more about the PEACE framework here: https://www.app.college.police.uk/app-content/investigations/investigative-interviewing/



INTERROGATION STYLE → INVESTIGATIVE INTERVIEW

GUILDFORD 4 (1975)
BIRMINGHAM SIX (1976)

ROYAL COMMISSION ON CRIMINAL PROCEDURE (1981)

POLICE AND CRIMINAL EVIDENCE ACT (1984) & PEACE

ROYAL COMMISSION ON CRIMINAL JUSTICE (1991)

7 PRINCIPLES OF INVESTIGATIVE INTERVIEWING & PEACE

CONFESSION DRIVEN → INFORMATION GATHERING

CREATIVITY AND CYBER SECURITY

DR DEBI ASHENDEN,
CRANFIELD UNIVERSITY

Understanding of cyber security risk has traditionally been driven by the engineering and physical sciences where risk is seen as knowable and measurable. In the next issue of CREST Security Review we will focus on cyber security, highlighting new research that shows that these risks aren't best addressed through technological innovation.

'Specimens of IT Fauna' is one example of this human-centred approach and is the result of collaboration between social scientists, designers and technologists. The aim of this project was to use critical design to encourage cyber security practitioners and policy makers to re-conceptualise cyber security risk and think about technology in new and different ways.

These artefacts demonstrate the way critical design can be used to reflect on our understanding of cyber security and to envision future risks in a creative way.

SPECIMENS OF IT FAUNA

The internet is ubiquitous, yet its detailed inner workings remain wrapped in mystery. We rely on a wide range of myths, metaphors and mental-models to describe and communicate the network's abstract concepts and processes. Packets, viruses, worms, trojan horses, crawlers and cookies are all part of this imaginary bestiary of software.

This new mythology is one of technological wonders, such as live streams and cloud storage, but also of traps, monsters and malware agents. Folk tales of technology, however abstract and metaphorical, serve as our references and guidelines when it comes to making decisions and protecting ourselves from attacks or dangers.

Between educational props and memorabilia, this series of objects visualises and celebrates the abstract bestiary of the internet and acts as a tangible starting point to discuss our relationship to IT technology.

The artefacts were produced as part of the Visualisation and Other Methods of Expression (VOME) project, which was funded by the UK's Engineering and Physical Sciences Research Council (Grant number: EP/G002347/1) and led by Debi Ashenden at Cranfield University.

01
Web-crawler

Scale 6:1
The Web-crawler (also known as web-spider or web-robot) methodically patrols the network to index its contents.

(1) STP Wire Cat 6E
(2) Crawler
(3) Content ="follow"

02
Low Orbit Ion Cannon

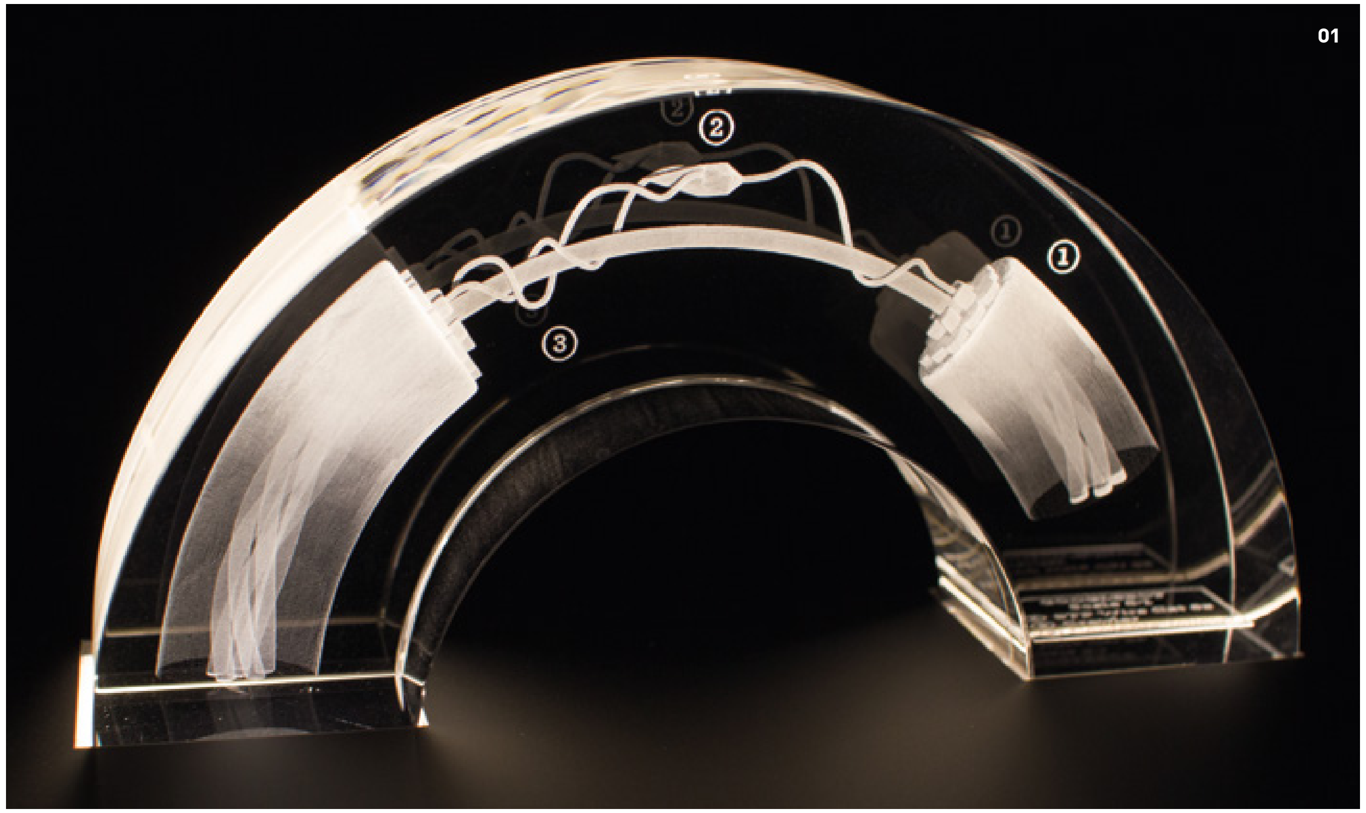
Scale 1:100.000.000
The Low Orbit Ion Cannon, is a powerful weapon in the video game Command and Conquer. It is also the name of a piece of software used to carry out denial of service attacks.

(1) Botnet Zombies
(2) Botnet Handler
(3) Attack Leader
(4) LOIC
(5) DDoS Target

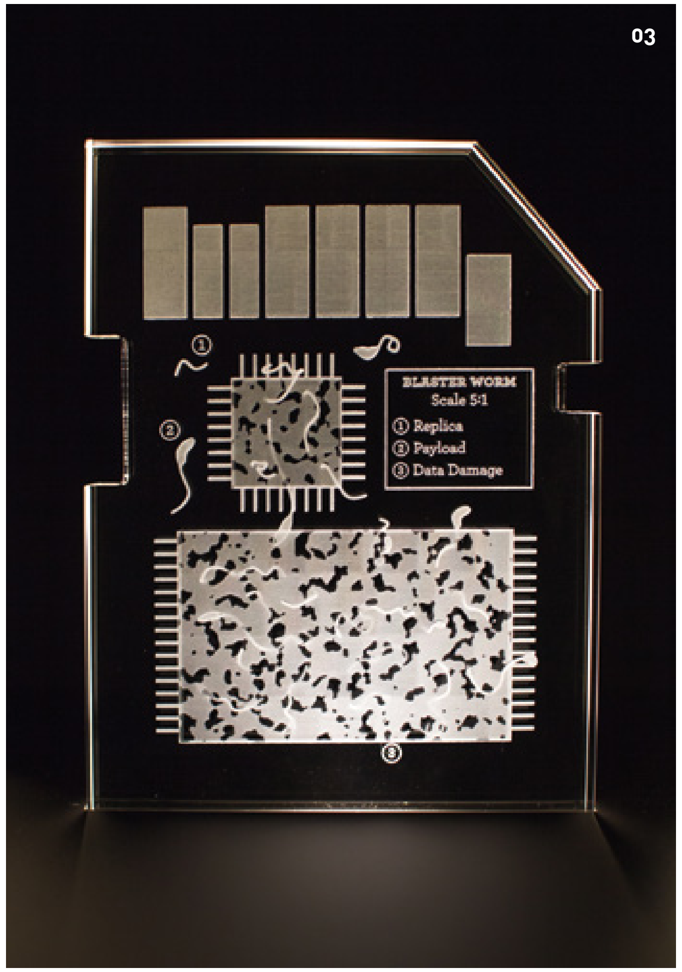
03
Blaster worm in SD card

Scale 5:1
Computer worms are standalone malware programs have the ability to replicate and spread their malicious 'payload' to other computers on a network.

(1) Replica
(2) Payload
(3) Data Damage

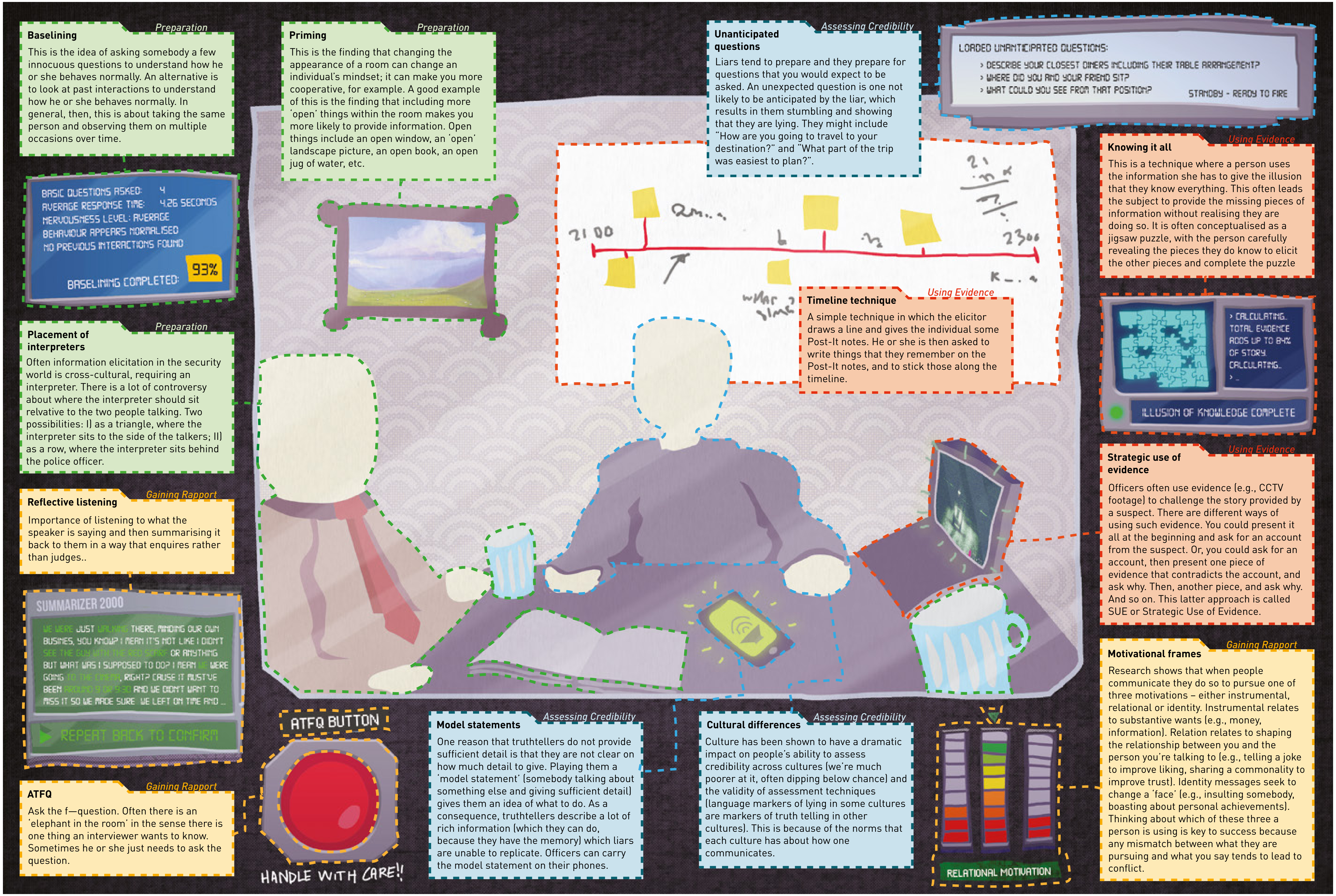

01

02


03

MIND MAP ON ELICITATION

WE CHART THE LAY OF THE EVIDENCE LAND



Preparation

Baselining

This is the idea of asking somebody a few innocuous questions to understand how he or she behaves normally. An alternative is to look at past interactions to understand how he or she behaves normally. In general, then, this is about taking the same person and observing them on multiple occasions over time.

BASIC QUESTIONS ASKED: 4
AVERAGE RESPONSE TIME: 4.26 SECONDS
NERVOUSNESS LEVEL: AVERAGE
BEHAVIOUR APPEARS NORMALISED
NO PREVIOUS INTERACTIONS FOUND
BASELINING COMPLETED: 93%

Preparation

Placement of interpreters

Often information elicitation in the security world is cross-cultural, requiring an interpreter. There is a lot of controversy about where the interpreter should sit relvative to the two people talking. Two possibilities: I) as a triangle, where the interpreter sits to the side of the talkers; II) as a row, where the interpreter sits behind the police officer.

Gaining Rapport

Reflective listening

Importance of listening to what the speaker is saying and then summarising it back to them in a way that enquires rather than judges..

SUMMARIZER 2000

WE WERE JUST WALKING THERE, MINDING OUR OWN BUSINES, YOU KNOW? I MEAN IT'S NOT LIKE I DIDN'T SEE THE GUY WITH THE RED SCARF OR ANYTHING BUT WHAT WAS I SUPPOSED TO DO? I MEAN WE WERE GOING TO THE CINEMA, RIGHT? CAUSE IT MUST'VE BEEN AROUND 9 OR 9:30 AND WE DIDN'T WANT TO MISS IT SO WE MADE SURE WE LEFT ON TIME AND ...

REPEAT BACK TO CONFIRM

Gaining Rapport

ATFQ

Ask the f—question. Often there is an 'elephant in the room' in the sense there is one thing an interviewer wants to know. Sometimes he or she just needs to ask the question.

Preparation

Priming

This is the finding that changing the appearance of a room can change an individual's mindset; it can make you more cooperative, for example. A good example of this is the finding that including more 'open' things within the room makes you more likely to provide information. Open things include an open window, an 'open' landscape picture, an open book, an open jug of water, etc.

Assessing Credibility

Model statements

One reason that truthtellers do not provide sufficient detail is that they are not clear on how much detail to give. Playing them a 'model statement' (somebody talking about something else and giving sufficient detail) gives them an idea of what to do. As a consequence, truthtellers describe a lot of rich information (which they can do, because they have the memory) which liars are unable to replicate. Officers can carry the model statement on their phones.

Assessing Credibility

Unanticipated questions

Liars tend to prepare and they prepare for questions that you would expect to be asked. An unexpected question is one not likely to be anticipated by the liar, which results in them stumbling and showing that they are lying. They might include "How are you going to travel to your destination?" and "What part of the trip was easiest to plan?".

LOADED UNANTICIPATED QUESTIONS:

› DESCRIBE YOUR CLOSEST DINERS INCLUDING THEIR TABLE ARRANGEMENT?
› WHERE DID YOU AND YOUR FRIEND SIT?
› WHAT COULD YOU SEE FROM THAT POSITION?

STANDBY - READY TO FIRE

Using Evidence

Timeline technique

A simple technique in which the elicitor draws a line and gives the individual some Post-It notes. He or she is then asked to write things that they remember on the Post-It notes, and to stick those along the timeline.

Assessing Credibility

Cultural differences

Culture has been shown to have a dramatic impact on people's ability to assess credibility across cultures (we're much poorer at it, often dipping below chance) and the validity of assessment techniques (language markers of lying in some cultures are markers of truth telling in other cultures). This is because of the norms that each culture has about how one communicates.

Using Evidence

Knowing it all

This is a technique where a person uses the information she has to give the illusion that they know everything. This often leads the subject to provide the missing pieces of information without realising they are doing so. It is often conceptualised as a jigsaw puzzle, with the person carefully revealing the pieces they do know to elicit the other pieces and complete the puzzle

› CALCULATING.
TOTAL EVIDENCE ADDS UP TO 84% OF STORY.
CALCULATING..
› _

ILLUSION OF KNOWLEDGE COMPLETE

Using Evidence

Strategic use of evidence

Officers often use evidence (e.g., CCTV footage) to challenge the story provided by a suspect. There are different ways of using such evidence. You could present it all at the beginning and ask for an account from the suspect. Or, you could ask for an account, then present one piece of evidence that contradicts the account, and ask why. Then, another piece, and ask why. And so on. This latter approach is called SUE or Strategic Use of Evidence.

Gaining Rapport

Motivational frames

Research shows that when people communicate they do so to pursue one of three motivations – either instrumental, relational or identity. Instrumental relates to substantive wants (e.g., money, information). Relation relates to shaping the relationship between you and the person you're talking to (e.g., telling a joke to improve liking, sharing a commonality to improve trust). Identity messages seek to change a 'face' (e.g., insulting somebody, boasting about personal achievements). Thinking about which of these three a person is using is key to success because any mismatch between what they are pursuing and what you say tends to lead to conflict.

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 80 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 its website at **www.crestresearch.ac.uk** and follow it on twitter **@crest_research**

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