CENTRE FOR RESEARCH AND EVIDENCE ON SECURITY THREATS

CREST DIGEST

Issue 1, Jan 2017

A round-up of research relevant to understanding and countering security threats.

CONTENTS

NEW RESEARCH

Popular lie detection technique comes under scrutiny

The Scientific Content Analysis or SCAN technique for detecting deception in written statements is used in several countries as an aid to investigation. The technique involves analysing the language used in an individual's written statement for specific criteria that the developer of SCAN claims are indicative of truthfulness or deceit. According to the developer's website, SCAN "will solve every case for you quickly and easily", and is an unbiased technique because it focuses on the subject's words and not "personality differences or ambiguous clues".

When deciding whether to adopt a technique like SCAN to detect lies, you need to be sure of two things:

- Does the technique accurately distinguish between truth and deception? Is the technique truly objective, or is its application and outcome biased by contextual information (validity)?
- Does the technique result the same outcomes when used by different (trained) people (reliability)?

Two more academic research studies led by researchers from the University of Maastricht have just been published, and build on a growing set of evidence that raises doubts about the validity, reliability and objectivity of SCAN as a lie detection tool.

Glynis Bogaard and her team (which included CREST researcher Aldert Vrij) elicited true and deceptive written statements from undergraduate students, and then had them scored independently by four raters who had received various degrees of SCAN training. There was good agreement between the raters about the presence or absence of SCAN criteria in the statements, but the SCAN criteria themselves did not discriminate truthful from deceptive statements. This study supports the reliability of SCAN under these circumstances but not its validity.

Separately, a team led by Miet Vanderhallen compared experienced SCAN analysts with detectives and undergraduate students assessing statements as deceptive or truthful. Students and detectives averaged around 80% of correctly classified truthful statements, whereas SCAN analysts scored average 54%. However, SCAN analysts scored better when it came to deceptive statements (78% correctly classified). This was significantly better than the students' performance, but not significantly better than the untrained detectives. The researchers also noted that SCAN analysts used non- SCAN criteria as well as SCAN criteria when making their judgements.

At best these studies call into question the 'added value' of using SCAN in investigative contexts. At worst, using SCAN might divert investigators away from more robust credibility assessment tools.

References

- Bogaard, G., Meijer, E. H., Vrij, A., & Merckelbach, H. (2016). Scientific Content Analysis (SCAN) Cannot Distinguish Between Truthful and Fabricated Accounts of a Negative Event. *Frontiers in Psychology* 7. http://journal.frontiersin.org/article/10.3389/fpsyg.2016.00243/abstract
- Vanderhallen, M., Jaspaert, E., & Vervaeke, G. (2016). SCAN as an investigative tool. *Police Practice and Research* 17(3):279-293. http://www.tandfonline.com/doi/full/10.1080/15614263.2015.1008479
- SCAN website: http://www.lsiscan.com

The role of trust in deciding which terrorist faction to join

When a terrorist organisation splits along ideological lines, how do members choose one faction over another? You might expect that these would be ideologically-based decisions. After all, involvement in a violent group is a high risk activity that demands high levels of personal commitment. It is logical to assume, therefore, if someone is prepared to take those risks and make that commitment, they will only do so if they believe strongly in the cause. A new article by John Morrison (University of East London) challenges that assumption.

Morrison examines individuals' decisions to side with one side or another during ideological splits in the Irish Republican movement that continued up to the 1997 split between the Provisional IRA (which chose a political route) and the so-called 'dissident' Republican groups that continued to pursue a violent path. Based on interviews with 43 Republican activists from a leadership figures to rank and file members, Morrison shows that when it comes to individual decisions to join one side or the other social commitment may trump – or at least compete with – ideological commitment. He writes: "The tipping-point for the majority came when they assessed how those individuals they trusted, and distrusted, were aligning. For many this was a significantly more powerful factor than any strategic or ideological divide."

And what was the basis of this trust? For many, those they trusted were family or people from their close community – people they had grown up with and with whom they had strong bonds. For others it was influential local figures, who often engendered more trust than more distant senior leadership figures.

Morrison also highlights the importance of trust in organisations' publications, citing the merger of An Phoblacht and Republican News and its allegiance to the PIRA as pivotal after the 1986 split between the PIRA under Gerry Adams and Martin McGuinness, and the Continuity IRA: "With these newspapers being the first port of call for the majority of members to gain access to political and paramilitary statements and interpretations of events this proved to be critical in the affirmation of the Adams/McGuinness leadership".

Morrison's findings add to our understanding of how and why individuals are attracted to terrorist groups, and chime with other research on the nature of commitment in terrorist groups (see, for instance, Horgan 2009). The findings are also consistent with research in organisational psychology that shows that local level relationships

matter more than relationships with distant leadership figures.

So, for a new recruit, it's often not ideological position that matters most, but who else is in the group. This insight also has implications for disengagement/deradicalisation programmes. If commitment is primarily social rather than ideological, then counter-narrative or ideological 'deprogramming' strategies won't help lure someone away from a group of individuals with whom he or she feels a close personal bond of trust.

References

- Horgan, J. (2009). Walking away from terrorism: accounts of disengagement from radical and extremist movements. NY: Routledge
- Morrison, J.F., (2016). Trust in me: Allegiance choices in a post-split terrorist movement, *Aggression and Violent Behavior* 28, pp 47-56 http://www.sciencedirect.com/science/article/pii/S1359178916300167

Can you tell if someone is pretending not to recognise a face?

Imagine the police are interviewing someone they suspect to be part of a terrorist conspiracy. The interviewee strenuously denies being part of the network. The police show him photos of people in that network and ask if he knows them. Each time he says no. Can the police tell if he is lying?

The results of a new study from researchers at Portsmouth and Southampton universities point to one promising method for doing this. Study participants looked at photos of people presented on a computer and stated whether they did or did not know those people. The photos included people that the participants knew well, famous celebrities, people whose photos they had studied earlier (but otherwise did not know), and unknown people. Sometimes the participants lied about whether they recognised the photos, sometimes they told the truth.

The computer's camera recorded participants' eye movements as they looked at the photos. Our eyes are always moving when we look at something, in tiny movements (or 'saccades') with brief pauses, called 'fixations', in between. We know that our eyes move in a different pattern, with fewer fixations, when looking at a face we recognise, compared with when the face is unfamiliar, and there is good evidence that this pattern is involuntary. In other words, it's hard to control or fake.

The research team found that their participants had fewer eye fixations when presented personally relevant faces and famous celebrities, compared to when they looked at photos of unknown people, even when they were lying about whether or not they knew the people in the photo. Lies about newly learned faces did not produce the same differences.

These findings point to measuring eye movements as one technique for detecting concealed recognition, though more studies are needed to strengthen the evidence base. To implement the technique in an interview context, the interviewers would need to compare their suspect's eye movements when looking at photos of the network when compared to people they were sure the suspect did and didn't know. The faces producing fewer fixations are likely to be the faces he recognises – whether he says so or not. Because the eye movements are involuntary it would be difficult to deploy countermeasures whilst appearing cooperative – although of course the suspect could just close his eyes or avoid looking at the photos at all. Recognising photos doesn't mean that the suspect is part of a terrorist network, of course, just that he is lying about not knowing other members of the network. Another potential limitation is that interviewers would be limited in how often they could show the same set of photos to the suspect – or they will become 'familiar faces' that he will recognise despite not knowing them previously.

Aldert Vrij is a CREST core programme lead, Lorraine Hope is a CREST core programme co-investigator,

and Anne Hillstrom is a co-investigator on a CREST commissioned project.

- Millen, A., Hope, L., Hillstrom, A., & Vrij, A. (2017) Tracking the truth: The effect of face familiarity on eye fixations during deception. *Quarterly Journal of Experimental Psychology*. Pre-publication full text: http://www.tandfonline.com/doi/pdf/10.1080/17470218.2016.1172093

SPECIAL ISSUE FEATURE

Complex and ambitious engineering efforts by violent non-state actors

The latest issue of the open access, peer-reviewed *Journal of Strategic Security* is devoted to articles on "complex engineering by violent non-state actors (VNSAs)", the output of a programme of work from a group of researchers associated with START, led by Gary Ackerman.

This collection of articles offers insight to the most ambitious activities of VNSAs, which are defined broadly to include terrorists, gangs, transnational criminal organizations, and insurgents. The overarching aim is to understand what resources and expertise are needed for a VNSA to develop and execute a complex engineering task, and case studies include Aum Shinrikyo's chemical weapons efforts and embryonic nuclear programme, PIRA's development of mortars, the FARC's 'narco-submarines', A Q Khan's nuclear proliferation activities, the Hamas tunnels, and the development by transnational organised crime organisation Los Zetos' development of a complex communication system across Mexico.

In the introduction to the issue, Ackerman explains that these complex engineering activities have in common a requirement for "multiple components (sub-tasks) of different types (e.g., mechanical, chemical, machining) that must integrate properly in order for the effort to succeed", "a variety of technical skills (such as chemical synthesis, welding, or electronics)", and teamwork to achieve the goal.

According to the existing research literature, factors that prompt VNSAs to innovate include a desire for status (within or among VNSAs), the imposition of security force countermeasures, the need to overcome 'desensitization' of those the group seeks to influence, and, in some cases a leader's 'techno-fetishism' (a fascination with sophisticated technology).

Organisational facilitators of innovation include being risk-tolerant, and a willingness to experiment and learn. Having an identified function responsible for 'engineering' or R&D also helps, whilst conflict within a VNSA hampers innovation. Specialist engineers don't necessarily have to be outstandingly talented, as long as they are competent, flexible, and around for a while. Unsurprisingly, VNSAs will tend to protect members with important and rare technical skills.

Each case study follows the same structure, which allows for a comparative analysis. Looking first at the trigger for and decision processes involved in each complex engineering effort, the case studies broadly support the findings from the existing literature. These VNSAs innovated first and foremost to overcome countermeasures from opponents, but also to gain status and publicity, and (in the case of Aum Shinrikyo in particular) to satisfy a leader's fetish for technology.

Experts involved in these activities were rarely 'home- grown' by the VNSAs, but tended to be trained professionals. Some volunteered, whilst others were specially recruited, hired as consultants, or even coerced by the VNSA. Materials were purchased through overt commercial channels, via the black market, or in a couple of instances from state sponsors (never stolen).

Examining how VNSA decisions to innovate are implemented (a topic on which there is scant existing academic research), the case studies suggest that several years of effort by a specialised R & D unit within the VNSA are needed to bring a complex engineering project to fruition. Significant investment of resources and expertise was evident in each case. For their activity to continue without being detected or stopped by the authorities, the VNSAs needed bases in operating environments

that were difficult or impossible for security agencies to penetrate. The long time scale also highlights the patience and determination of these organisations – all of whom faced major setbacks but persevered regardless – and their openness to experimenting and learning.

Overall, these articles avoid painting their subjects as movie-plot 'supervillans' whilst nevertheless highlighting the "genuinely impressive" engineering achievements by these groups. This signals that we should be wary of dismissing as 'scaremongering' the potential for serious harm through the development and exploitation of new technologies by hostile groups.

The authors present their research as exploratory, offering potential foundations on which future research can build, and in the final article Ackerman sets out a series of research hypotheses. A programme to test these could yield important insights relevant to policy and practice in countering terrorism and organised crime. As Jez Littlewood explains in his preface to the issue, greater understanding of a VNSA complex engineering task may help police and intelligence agencies "to make that task more difficult through the identification and manipulation of choke points, development of additional obstacles for the VNSA– resources, materials, personnel, risk of detection– and making the overall operational environment more conducive to the tactical failure of the undertaking and/or weapon for the VNSA".

All articles are freely available via: http://scholarcommons.usf.edu/jss/vol9/iss1/

Table of contents

OTHER ARTICLES THAT CAUGHT OUR EYE

Techniques for establishing rapport

In a study of how rapport is developed in official police interviews, 123 police interviewers were interviewed about rapport-building techniques they used with high- value interviewees. Interviewers reported that the most commonly used techniques were creating a sincere and likeable impression (through establishing points of similarity with the interviewee and the use of humour) and using the norm of reciprocity (when someone receives something, they feel an obligation to give something in return).

References

- Goodman-Delahunty, J., & Howes, L. M. (2014). Social persuasion to develop rapport in high- stakes interviews: qualitative analyses of Asian- Pacific practices. *Policing and Society*, 1-21. http://www.tandfonline.com/doi/full/10.1080/10439463.2014.942848 (open access)

Social networking and phishing attacks, and a game to avoid phishing

A series of studies with large companies highlights the vulnerability of employees who use social networking sites (SNS) to phishing attacks. In a field experiment, the researchers showed that the detail employees provided on SNS allowed them to be easily deceived by a hostile posing as a friend or associate. Interviews with Chief Information Security Officers revealed that organisations had weak policies on SNS use. The researchers suggest that "SNSs have become important security holes where, with the use of social engineering techniques, malicious attacks are easily facilitated".

- Silic, M., and Back, A. (2016). The Dark Side of Social Networking Sites: Understanding Phishing Risks. *Computers in Human Behavior*, 60, 35–43 http://www.sciencedirect.com/science/article/pii/S0747563216301029

Another study reports on the successful trial of a mobile game, developed as tool to educate users about the risks of phishing attacks. The study results showed that after playing the game people showed more awareness of the threat and an increased motivation to take actions that would help them avoid phishing attacks. They also commended the game for being more fun and engaging than books or articles. This was a small scale study, and although the results are encouraging, the researchers admit that more development and testing will be necessary before it can be recommended for widespread use.

References

- Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*, 60, 185-197. http://www.sciencedirect.com/science/article/pii/S0747563216301236
- For a basic introduction to phishing, see our CREST guide here: https://crestresearch.ac.uk/resources/introductory-guide-phishing/

BEYOND THE PEER-REVIEWED LITERATURE

Reports from journalists, researchers, think tanks and governments

Milestones to militancy

A publication from the Centre on Religion & Geopolitics (part of the Tony Blair Faith Foundation) examines the careers of 100 prominent violent Islamist extremists (they use the term 'jihadis'). The authors (Mubaraz Ahmed, Milo Comerford, and Emman El- Badawy) suggest that their analysis sheds light on the potential jihadist leaders of tomorrow.

The research is based on a non-random sample of 100 'jihadis' from across the Middle East and Africa, many of whom had been active for generations. There is no control sample (a comparison group of individuals with similar backgrounds who did not join the jihad) so the results are purely descriptive.

The results are largely in line with most similar studies - for instance, they found no 'typical' jihadi profile. Some of those in this sample may have also been included in similar case study research (e.g., Sageman 2004), so the current research might be better characterised as a partial replication of previous work, rather than completely new evidence.

The more interesting part of the analysis highlights the significance of personal connections and links often made in theatres of war and/or prison. Whilst not new, it illustrates the importance of social ties – and the places where such ties are forged – in the development of a terrorist career (see also the discussion of Morrison 2016, in this issue).

The authors' recommendations take quite a leap from the results of the study. Many are obvious, some will be controversial ("compulsory religious education programmes for inmates convicted of jihadi-related offences") and others are vague ("Universities should incentivise students from all disciplines to attend modules that build skills

to critically analyse texts on social and political issues.")

- Ahmed, M., Comerford, M., & al-Badawy, E. (2016). Milestones to Militancy: What the lives of 100 jihadis tell us about a global movement. *Centre on Religion & Geopolitics*. Available: http://tonyblairfaithfoundation.org/religion-geopolitics/reports-analysis/report/milestones-militancy
- Sageman, M. (2004). *Understanding Terror Networks*. University of Pennsylvania Press

FEEDBACK

If you would like more detail, or have suggestions for improving CREST Digest, please let us know via https://crestresearch.ac.uk/contact/. For updates on new research, follow us on Twitter at: @crest_research