Culturing Defensive Immunity: Hardening Psychological Targets Against Cyber Attack

Mils Hills and Guy Batchelor
Northampton Business School, UK
mils.hills@northampton.ac.uk
guyb73@me.com

Abstract: Academics in business science and elsewhere have begun to look at what Vaughan (1999) called the "dark side of organisations" and started to engage with the fact that people connected to cyber systems can be the source of great opportunity for exploitation. MacGillivray (2014) notes that organisations should be seen as socio-technical: where infrastructure and systems shape and are shaped by the people that work with them. The current paper puts these socio-technical systems at the heart of cyber-attack and defence - where we see 'cyber' as being shorthand for any computer-dependent technologies used to achieve dark effects on the human mind and subsequent behaviour (e.g. SMS received on a mobile phone).There is no logic to restrictively focussing on user behaviour around laptops and desktops. This paper provides some unconventional examples of cyber-attack. Our concern is with enabling decision-makers (or those supporting them) to challenge their assumptions about information received, adjust behaviours accordingly and thereby render them and their organisations increasingly resilient to the efforts of creative adversaries, no matter whether those adversaries motivation is commercial, political or personal. From such target-hardening arises organisational competitive advantage.

Keywords: psychological, target, immunity, trap, culture

1. Introduction

A challenge for any organisation – commercial, public sector or military – is to detect meaningful alterations within (or affecting) their decision-making people and processes. Drawing on insight from the British Army – whose forces constantly review a planned mission through the use of the military estimate tool ('Seven Questions'), our notion is that it should become intuitive to persistently ask 'Has the situation changed?'[1]Indeed, the core message of this paper is that organisations must become adept at embedding this self-questioning into the fibre of their security and other practice, because cyber-threats (as a blend of the ingredients of human ingenuity and computer-enabled communication) are designed to bait or trigger psychological traps (cf. Hammond, Keeney and Raffa 1998). These traps encourage targets to either continue with, or cease, courses of action: to deceive individuals into the peril of believing that reality has (or has not) changed by manipulating situational awareness.

Decision-makers, especially under conditions of "time constraints, limited and often ambiguous information, intense pressure, and often stark conflicts of interest" (MacGillivray 2014: 1719), seek to find easy ways to process of complex situations. We may, for example, trust a source of information because we have previously trusted it; adopt an idea because we have recently heard it or dismiss information which does not accord with our assumptions because we do not like it. At the level of board decision-making or in a vital function of a business: these errors can be extremely costly. We suggest some ways in which these errors can be rehearsed away from being so tempting. It will also be important for individuals to become cognisant of the fact that mindsets, attitudes and commonsense may be affected when they move between the thought-processes and places of being 'at work' and 'on personal time'. The worldview of individuals needs to be adjusted to reflect that, just as we are never 'off duty' when connected to the office via phones, tablets and other tech – so too as employees guarding an organisation's Intellectual Property (IP), reputation or other value - we are never 'off duty' as potential targets.

At the personal level, and decision-makers may well be precisely targeted when situational awareness is low, even government Ministers can be easily tempted into providing intimate photographs to a Twitter correspondent leading to the potential for blackmail. In other real world events a USB drive is picked-up and taken into a corporate data centre by all employees who spot it; spoof news stories go viral within moments; spear-phishing attacks and fake dating profiles scam the security conscious and hopelessly romantic alike – all of these and more represent successful positioning and execution of psychological traps via cyber means. This

[1] Full information on the Estimate process available in British Army doctrine, here: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33695/ADPOperationsDec10.pdf

paper will briefly describe the individual impact of some cyber-attacks and thereby extend discussion in terms of how these *could* have generated even more acute organisational impact.

The approaches we set out to enhance organisational resilience to decision-targeting hold true for both individuals and organisations, indeed each depends on the other to attain and sustain an appropriate security culture. As we bring this paper to a conclusion, the fallout of the behaviour of two former Foreign Secretaries in the UK continues to cause ripples. Attending a meeting called by journalists purporting to represent a Chinese company, the then chair of the powerful House of Commons Intelligence and Security Committee (and board member of private security companies) has resigned his Committee role and will stand down from Parliament at the next election. The entire scandal having been facilitated by computer-mediated communications and psychological playfulness.

Having first set out a sense of the scale of the challenge, the authors will finally sketch a practical approach to hardening psychological targets. We describe early ideas for embedding an awareness and openness in individuals to constantly question whether their world-view remains accurate. Shock and surprise are the enemy of any system – vigilance to changes in the internal or external ecosystem is vital, yet difficult to attain. Being able to sustain such vigilance is, again, a form of *competitive advantage*. In addressing the major forms of decision-making psychological traps – we propose ways in which organisations can implement an enhanced approach to security culture that builds (through repetition) psychological immunity to malign intent. Our key ambition is to present some concepts which will enable leaders and managers to enhance their organisation and people's resilience to influence by cyber means. From enhanced and accurate situational awareness, organisations will also increase their ability to take good risks: individuals must be empowered and enabled to make constructive use of the Internet and the opportunities that it can provide – perhaps the realisation that one can 'hide in the open' can help balance security with presence.

2. Defining terms

This section moves towards a working definition of 'cyber-security'. This is a term which, as with so many, is bandied-around in media, academic and other discourse in imprecise ways. Our core interest is in people (the human factor) and viewing them as (a) needing to be protected from influence and (b) prevented from damaging the systems and processes around them (whether unwittingly or otherwise).

A recent report on cybersecurity (commissioned from the Institution of Engineering and Technology by the UK government's Centre for the Protection of the National Infrastructure – CPNI) informs us that:

> *One internationally agreed definition for cyber security is 'the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets' (IET 2013: 14).*

This definition is taken from one advanced by the International Telecommunications Union (ITU)(an agency of the United Nations) in 2009. Even the kindest observer would concede that this all-inclusive definition is not the most helpful. It is so embracing that everything is covered. Indeed, in a 2014 article, Craigen, Diakun-Thibault and Purse noted that the term 'cybersecurity' "is used broadly and its definitions are highly variable, context-bound, often subjective, and, at times, uninformative. There is a paucity of literature on what the term actually means and how it is situated within various contexts" (2014: 13).

Indeed, we are even more bold: many of the learned and practitioner discussions about 'cyber' matters are almost entirely context-free, and in general descriptive and often vapid. Cyberspace really means 'somewhere out there' in a place here computers eventually connect (like a strange distant synapse). We argue that *cyber* must be thought of in a much more concrete way. Cyber-security is the countering of the means by which an end can be achieved – the persuasion of human targets to do something that they should not through (either or both) socio-technical means.

Whilst Craigen*et al*. draw on a dictionary definition of cyber – unfortunately this does not really help: "'Cyber' is a prefix connoting cyberspace and refers to electronic communication networks and virtual reality (Oxford, 2014)". This definition captures all uses of the term 'cyber' (which is the point of a dictionary!), but it does not help work out what either cyber-security or cyber-insecurity, are. Although cyber is 'out there' – the effects are felt in or achieved through the human brain and the actions it takes. All that cyber is, is a means of – via computer-dependent media – communicating. The unhelpfulness of thinking of 'cyber' and its (in)security as being about cyberspace, computers, virtual reality and so on is that it generates an idea that cyber is about computers *per se* rather than things which *involve* computers at some point. Effects in or from computers may well be achieved by air-gapped humans inspired to do something as a result of information communicated via computers or through computer-dependent systems (e.g. mobile telephones). Alternatively, air-gapped humans may be persuaded to do something that threatens cybersecurity solely by another human.

From the authors' extensive experience in the public sector (government, military, law enforcement) and the private sector (up to and including boards and directors of security) – these viewpoints are just not held deeply nor strategically enough. Organisations may plan for business continuity triggers in the form of system outages or data corruption – but not for these other eventualities where systems are a means to an end of disrupting, thwarting or diverting decision-making. This may, we might speculate, simply be because the age profile of those at senior management and thought-leadership levels does not make it easy for them to acknowledge the relevance of cyber beyond conceiving of 'it' as just another type of infrastructure or technology. And yet one of the underpinning beliefs with which the authors have approached drafting this paper is that it is dangerous to think in this way. Hence, we contradict definitions of cyberspace such as the following:

> *the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where… people are linked together to exchange ideas, services and friendship (Public Safety Canada 2010).*

Although 'cyber' is indeed a global commons (like the oceans and the atmosphere), it is neither a world nor a virtual world. It is a technology which constitutes and is constituted by us, barely understood, in which communication can be achieved and availability to which is vulnerable to electronic as well as kinetic and other forms of attack. It enables markets, control systems, data, dating and many other functions to operate. But these markets, for example, do not exist any more than a roulette wheel exists on a virtual gaming table.

'Cyber' bridges hard and soft systems, yet the alarming fact is that there are many attempts being made to limit cyber-security to some kind of static concept which sounds much more like the approach one would take to physical security in the past: "Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption" (Lewis, 2006). This is an extraordinarily limiting idea – because it neglects the fact that any technical system is inevitably *socio*-technical because they are created, managed, used and abused by humans. Computer networks and databases (etc.) do far more than just *hold* information subject to being destroyed or damaged: they enable decisions. Systems may be entirely intact, technically 'secure' and yet still enable a well-crafted Tweet, email, SMS, fake What's App exchange, idea or other artefact to transit over them and have an effect on a decision-maker or their advisor(s). Lewis' definition is really referring to network or system security – a sub-set of the overarching topic area.

3. Cyber-scenarios: Recent events where decision-making has been influenced

The following section provides some illustrations of where cyber (i.e. computer-enabled) communications have interfered powerfully with individual or organisational decision-making / judgment. This has been achieved by the manipulation or determination of situational awareness, i.e. the understanding of the world around the individual. We begin by presenting some useful definitions of situational awareness. The term is drawn from the study of pilots and their fast and pressured decision-making. Whilst most people will be familiar with Boyd's OODA (Observe, Orient, Decide, Act) model –most will not be aware that Boyd was a USAF fighter pilot.[2] Endsley, therefore, defines Situational Awareness (SA) as "the pilot's internal model of the world around him at any point in time" (1988) – this model being synthesised from what the instruments report, what can be seen outside, what radar and other sensors show as well as sensory input, the benefits of memory, experience and so on.

Endsley has later provided us with the useful view that SA provides "the primary basis for subsequent decision making and performance in the operation of complex, dynamic systems" (1995). Given the pace with which business is conducted and the way in which reputation, advantage and market share can be won or lost (in the private, public and military theatres) – these appreciations of SA are valuable. Success in commerce, administration and conflict is all about managing complex, dynamic systems. Another way of describing SA is through the use of the anthropological concept of the *worldview* – the internal model of how and why the individual and their socio-technical world works. When one thinks of a target's situational awareness as a

[2] A useful reading on this topic is: http://www.fastcompany.com/44983/strategy-fighter-pilot

‘worldview’ – it becomes more readily apparent that it is possible to model and understand the target – through using empathy and psychological and cultural collateral to actively or passively establish a view of that target and how and why they do what they do.

The following vignettes provide examples of the kinds of perils that we would wish to equip individuals and organisations to suspect, detect and avoid in an irresistibly dynamic and open world.

a. Willygate: Ministers in the mangle

> *"Late at night, I began a series of flirtations in response to approaches from women on social media. Deep inside, I knew I was playing with fire. Now it has consumed me and my family" - Brooks Newmark MP (BBC News online 12 October 2014).*

It proved surprisingly easy for a journalist to persuade a junior Minister (Brooks Newmark MP) to send explicit photographs of himself to a Twitter correspondent who was someone very different to who he had assumed (hoped) they were. As BBC News puts it:

> *he had sent pictures to a freelance reporter, who adopted the false identity of "Ms Wittams" and described himself on Twitter as a "twenty-something Tory PR girl". "Sophie" then contacted and interacted with a number of Conservative MPs via the social networking site (Ibid.).*

With a very brief back-story on ‘her’ Twitter profile, a freelance reporter found that a Minister was amenable to both conversation and, within a short period of time, exchange of photographs via this cyber-link. This is hardly the most sophisticated, nor novel, type of way of causing embarrassment to politicians or other middle-aged men. What is, perhaps, slightly more surprising, is that this was so easily achieved in an ever more ‘security conscious’ world, replete with warnings about the easy exploitation of social media.

Our intention in this paper is to push speculation further.

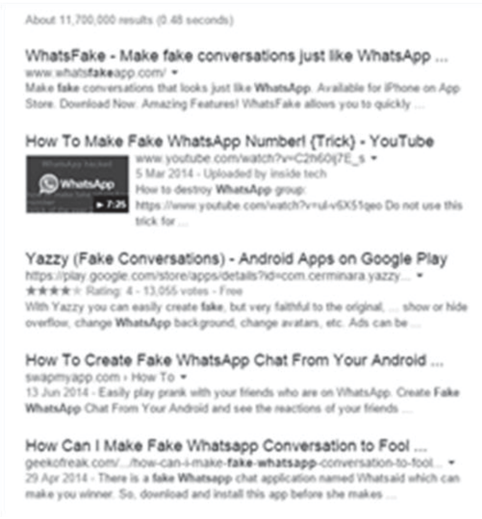
If it was *so* easy to detect and exploit a very conventional vulnerability in a figure in public life –we can reasonably assume that senior individuals in other walks of life may be just as (if not more) vulnerable. The effect sought in the Newmark case was clearly to generate business for a freelance journalist – but what if the effect sought were different? There is no reason why Newmark, a director of procurement, head of security of any other senior or middle-ranking individual might not be targeted on behalf of commercial rivals or others. If, rather than being motivated solely by generating embarrassment and media coverage in the very short term, Newmark’s behaviour (or that of a procurement, contract, facilities or other director or manager) had led to their being retained as an asset - what they might be pressured to do? For example, the threat of exposure could be leveraged by a criminal enterprise or others to award a contract to an uncompetitive bidder, re-open or close a regulatory investigation, endorse a product or service by attending functions or, simply, allow access to a site or a system by an unknown person.

Twitter, or email, or SMS or some other computer-enabled (i.e. cyber) communications can, then, produce devastating effects on an individual but also, potentially, to the organisations in which they work and the integrity and security of their processes. The next section will extend the awareness of the reader to an even more unusual phenomenon which, whilst being dependent on the existence of cyber-technology, does not actually use it directly.

3.1 Paper meets WhatsApp

The authors are aware of a case where a long-standing employee in an organisation is being investigated (and may well be dismissed) on the basis of a WhatsApp interaction. This in itself is not surprising – but what is mindboggling is the fact that the employee and employer only have possession of screen-shots of the interaction and that the evidence itself contains signs that it is hardly likely to have been conducted by that employee.

In short, the employee faces dismissal on grounds of gross misconduct (based on the content of the interaction) solely because the employer has reasonable belief that the interaction that the screenshots represent is real – and, we judge, because it fears the reputational and other effects of the allegations becoming public. It is easier to treat the artefact as true than try and establish that it may not be.



About 11,700,000 results (0.48 seconds)

WhatsFake - Make fake conversations just like WhatsApp ...
www.whatsfakeapp.com/
Make **fake** conversations that looks just like **WhatsApp**. Available for iPhone on App Store. Download Now. Amazing Features! WhatsFake allows you to quickly ...

How To Make Fake WhatsApp Number! {Trick} - YouTube
www.youtube.com/watch?v=C2h60tj7E_s
5 Mar 2014 - Uploaded by inside tech
How to destroy **WhatsApp** group:
https://www.youtube.com/watch?v=ul-v6X51qeo Do not use this trick for ...

Yazzy (Fake Conversations) - Android Apps on Google Play
https://play.google.com/store/apps/details?id=com.cerminara.yazzy...
★★★★☆ Rating: 4 - 13,055 votes - Free
With Yazzy you can easily create **fake**, but very faithful to the original, ... show or hide overflow, change **WhatsApp** background, change avatars, etc. Ads can be ...

How To Create Fake WhatsApp Chat From Your Android ...
swapmyapp.com › How To
13 Jun 2014 - Easily play prank with your friends who are on WhatsApp. Create **Fake WhatsApp** Chat From Your Android and see the reactions of your friends ...

How Can I Make Fake Whatsapp Conversation to Fool ...
geekofreak.com/.../how-can-i-make-**fake-whatsapp**-conversation-to-fool...
29 Apr 2014 - There is a **fake Whatsapp** chat application named Whatsaid which can make you winner. So, download and install this app before she makes ...

And yet, a simple search of Google reveals just how easy it is to find the software to enable fake WhatsApp (and other) conversations to be created (see left). But such an example encapsulates the power of cyber-attack which earlier restricted views of cyberspace and cybersecurity cannot engage with: in the hands of a creative and determined individual, an attack can be made on an individual / organisation that mat depend on leveraging awareness of the sensitivity of institutions to wrong-doing in their ranks, a cultural or other reluctance or inability to pursue the appropriate (but complicated) way to resolve the matter and a keen appreciation of where and what triggers are in organisations such that they have little choice but to over-react or react when they should not.

Here, then, the situational awareness of the employer is absolutely determined by the attacker(s). A worldview has been created that the employer is choosing to resist challenging. The employee, meanwhile, faces the significant challenge of defence against a physical copy of a digital interaction, where he is unable to access the originals and where the employer has no understanding of the technical issues and no appetite to get to grips with them.

4. The desired outcomes of cyber-attack

In this section, we wish to briefly outline some of the effects that cyber-attacks can have on decision-making. In essence, because humans seek (normally sensibly) to make life as efficient in terms of energy invested as possible – we look for reasons to continue believing in something rather than refuting it: unless we have our senses alerted by a particular experience or because we have reason to be on our guard. The Internet dater who has had some less than perfect experiences, for example, may be a good deal more suspicious than the naïve, possibly desperate, lonely heart. The skill of those behind effective cyber attacks, then, is to ensure that there are no easily perceived reasons by those targeted or hosting the target to challenge their activities OR provide absolutely compelling evidence that a perception or course of action must be changed OR inject enough uncertainty into a decision-making process that inaction and delay are inevitable.[3]

There are very simple rules which are designed to allow humans to avoid investing time and energy into thinking about a situation unless necessary. We default to look for patterns that confirm that a new situation is just like a similar one. Information which does threaten these patterns is likely to be dismissed – unless an organisation or individual has implemented challenge into its operating procedures. Decision-makers - especially under the conditions that MacGillivray described above (*op. cit.*) - seek to find easy ways to make sense of complex situations. Even when the situation is not one of crisis, as humans we default to imposing what we think are sensible, proven and unproblematic interpretations of our context. Hammond, Keeney and Raffa(1998) developed a summary set of such psychological traps. In the table below, we add a column paraphrasing the impact of these traps on assumptions of situational awareness:

[3] In future work, the authors intend to also cover the fact that cyber-attacks can undermine the control of the 'eight wastes' of Lean Management, both literally and metaphorically. By, for example, casting doubt on the integrity of content and integrity of an organisation's systems – normal information processing tasks can be rendered inefficient in the same way that defective items on a production line extract time and money if rework / recall are needed.

Type of Trap	Impact	Example
Anchoring	We assign disproportionate importance to the first information received	An overheard discussion or passing comment in a newspaper defines the topic / concept. Use of stereotypes.
Status Quo	Despite the existence of better alternatives, we commit to continuing the current course of action	Less psychological risk by sticking with what we know, taking action requires exposure to risk & its consequences. Research indicates that as option increase, the 'pull' of the status quo also rises.
Sunk Cost	Because we have already committed resources, we must continue	Reluctance to divorce from poor past decisions. Firing a bad employee threatens perceptions of your judgment in hiring them in the first place.
Confirming Evidence	Seeking information that justifies existing decisions rather than supporting alternatives	Bias in information sought and its interpretation. Weighting of confirming over opposing information, despite the alternatives being undeniable (e.g. scientifically valid).
Framing Trap	By misunderstanding what the problem is, our decisions are increasingly irrelevanr	Presentation of a problem shapes what traps become tempting, e.g. highlight sunk costs.
Overconfidence	We are over-optimistic about data and decisions	Range of possible outcomes narrowed because of false confidence in accuracy of assessment of what could happen / scope of problem.
Prudence	Risk averseness	Default to over-caution, especially when faced with significant decisions.
Recallability	Recent, dramatic events condition the response.	Something that has recently befallen or benefitted another gains [undeserved] priority and distracts from actual priorities.

(adapted from Hammond, Keeney&Raiffa2006).

In addition, these traps can inter-relate and affect one another. , the authors provide the examples of a:

> *dramatic first impression [that] might anchor our thinking, and then we might selectively seek out confirming evidence to justify our initial inclination. We make a hasty decision, and that decision establishes a new status quo. As our sunk costs mount, we become trapped, unable to find a propitious time to seek out a new and possibly better course. The psychological miscues cascade, making it harder and harder to choose wisely (Ibid.).*

These traps are related to cognitive frames: ways that come to shape how we perceive reality. Frames are heuristic thinking tools – where we hold an agenda or worldview that determines our attitude to specific and related issues. These frames (freed from challenge by mind guards and critical thinking) are problematic: "[f]or the most part, our use of frames is unconscious and automatic—we use them without realizing it" (Lakoff 2006: 9). It is this unconscious and automatic use of frames (e.g. the absence of suspicion about a change or lack of change in a situational picture) which is at the root of the means of hardening psychological targets against cyber-attack.

5. An emerging solution to harden psychological targets

The authors of this paper are motivated by their personal insight into the traps mentioned and the belief that something positive and concrete can be done to reduce the risk of them being exploited. We are part of a cluster of practitioner-researchers developing concepts to provide organisations with competitive advantage from novel, pro-active ways to engage with insider threats, embedded risks and other unconventional security challenges. Output from this cluster is referenced in this concluding section and indicated by an asterisk after the appropriate reference.

The need identified in this paper is for individuals and their organisations to challenge their understanding of their worldview / situational awareness. This is a key component of the question 'Has the situation changed?' and traditionally fundamental to intelligence analysis:

> *truly effective intelligence must on occasion be "doubting" of the enterprise at hand. It must raise difficult – and perhaps unpleasant – questions of operational planners. It must be free to inject contrary evaluations of the operational situation. It must not fall victim to – nor encourage – wishful-thinking or a raft of other misperceptions and biases in stressful situations (Dearth: 1995: 9).*

Drawing on our background in, respectively, strategic consultancy with the British Government and private sector and a distinguished career in the UK special forces community - we argue that organisations need to ensure that challenge is fundamental to any organisation's assessment of and assumptions about the world, driven by cyber or other means.

We think that existing approaches to hardening the human factor targeted through cyber means (whether more or less 'technical' in nature) are insufficient. We assume that employees in even the best communicated-to and compliant companies will not yet be hardened against psychological attack. This will be of particular concern to industries, individuals and organisations which fall within the targeting parameters of adversaries likely to behave in unconventional or unrestricted ways (where no technique is off limits).

Our proposal is for a portfolio of techniques which organisations seeking competitive advantage would adopt, embed and use to test their level of hardening against cyber-attacks. These extend from implementing systems which enable the ready sharing of information which might be relevant, gathered and interpreted by a dedicated team who can feed back to, report to appropriate structures within the organisation and reward the source of the original disclosure. Just as suggestion-boxes can be an incredibly cost-effective way of finding solution to improve productivity and cut costs in production lines (see Robinson and Schroeder 2009 and Curtis 2015*), so listening to 'front-line ideas' (as Robinson and Schroeder describe them) could also be a valuable source of intelligence from which to build more corporate immunity. In other words, to increase the ability of an organisation to learn from what may be happening to and around it; to empower more sensors to provide data to be processed, rendered into intelligence and considered as part of the approach by which individual and collective security and risk profiles and awareness are adjusted.

In his work tailoring and implementing lean approaches into a major manufacturing facility, Curtis (2015*) has achieved significant results by ensuring that all employees are genuinely involved in designing change and improvement processes. By investing considerable time and resources, Curtis has unlocked the problem-detection and -solving capabilities of his workforce, delivering cost and efficiency savings and also educating, engaging and raising the morale of that workforce. There is no reason why cyber- and other forms of security cannot be tackled in exactly the same commercially savvy way.

The precise means by which the collecting and collating of weak signals and early warning together will need to be adapted to the precise organisational environment of a business or other institution. Research such as that conducted by Anjali (2015*) makes concrete steps towards frameworks against which organisations could plan to gather and make sense of such information. Anjali also notes the role for nudge and other behavioural science approaches to develop a more effective means of achieving compliance with generic security protocols – such as overcoming human curiosity about a USB stick found outside a data centre.

Drawing on insights gathered from a very highly applied environment, Macfarlane and Maharajan (2015*) have begun to describe how the implementation of strong and protected, no-blame alternatives to traditional whistle-blowing mechanisms / tribunal cases inside organisations could also boost the situational awareness of boards and enable them to access up-to-date insight. Individuals would feel able to pass on information about wrongdoing in the workplace with no risk of retribution and, in an alternative scenario, have trust and confidence to report what they believe might have been an attempt to compromise them in their private life. The organisation would then provide support and care at the level of safety, security and well-being such that the employee gains confidence that s/he is protected and the organisation is able to issue guidance to others and amend its decision-making / testing of other sources and systems accordingly.

At all levels of an organisation, we recommend the more generalised use of 'red-teaming' to challenge assumptions and embed a questioning of 'Has the situation changed?' in the form of suspicion, even cynicism, about the ongoing value of a situational awareness assessment. Individuals should be coached to be self-reflective around whether they are falling foul of heuristics / psychological traps. The authors endorse the approach to implementing critical thinking that Moore (2015*) is developing – albeit originally for a very different purpose, countering radicalisation / grooming in schools. So, too, boards and those that advise them should expose themselves to the challenge represented in scenario-driven exercises (SDEx) (cf. Hills 2015, forthcoming). From the repeated use of high-impact, low-cost activities such as this, organisations and the systems that sustain them can increase their ability to suspect manipulation and more effectively detect and manage the consequences of being manipulated by others.

However, enhancing the ability of boards, heads of corporate security, human resources, IT and other departments to detect and decide on relevant actions to take requires, in our view, new forms of training and mentoring. Batchelor (2015*) argues that there is merit in drawing on the mental processes and disciplines of the special forces soldier – those individuals required to make frequent and important decisions under pressure and with incomplete and inconsistent information. Through immersive and other training, organisations and their individuals (high-profile and otherwise) can grow their competence for personal and corporate mental safeguards to stop individual lapses in judgement.

Additional approaches would include the potential use of 'tiger teams' who would attempt to use creative techniques to overwhelm or influence individual targets in an organisation – in much the same way that 'ethical hackers' attempt to subvert security systems. The difference here being that the attempts would be targeting psychological security as much as technical / physical security. No doubt there would be problematic issues raised if, for example, an executive did accept a bribe offered by an 'ethical tiger team' – the organisation would have detected a vulnerability that an adversary / other could have exploited. How the organisation chose to deal with such an eventuality would require consideration. As always, however, it is better for the threat to be detected by the employer than by a competitor.

Lewis (2015*) has taken this approach to the very grassroots level – in applying military and other approaches to detecting insider threats to a contentious small business sector (using animals). In this context, activists and others use a range of methods to build trust in often very low-tech ways. However, the insights gained from this research are useful as the exploits – being social in nature – could be undertaken via cyber means.

These vignettes of current research and conceptual development underline some sources of insight that could be drawn upon to harden psychological targets in organisations. Growing the immunity, resilience and protective questioning of employees at all levels of an organisation to cyber attack is a potential source of great competitive advantage to individual companies, industry sector and nation states. Achieving this target hardening is not easy – but neither is it impossible.

References

Anjali, *Cyber-security: A Pragmatic Approach to Preventing and Mitigating Insider* Threat, MBA Dissertation, Northampton Business School, University of Northampton, January 2015.

Batchelor, G *A Unique Leadership, Management Consultancy Drawing on a Special Forces Background*, MBA Dissertation, Northampton Business School, University of Northampton(forthcoming) April 2015.

BBC News online, *Brooks Newmark quits: MP says he is 'battling demons'*, 12 October 2014, http://www.bbc.co.uk/news/uk-politics-29586898

Craigen, Diakun-Thibault and Purse, *Defining Cybersecurity*, Technology Innovation Management Review, October 2014

Curtis, S *Front-line Thinking, Change and Lean Management*(working title), MBA Dissertation, Northampton Business School, University of Northampton(forthcoming) April 2015.

Dearth, D, *Strategic Intelligence: Theory and Application*, US Army War College / DIA (1995).

Endsley, MR.,*Situation awareness global assessment technique (SAGAT)*, paper presented at the National Aerospace and Electronic Conference (NAECON), Dayton, OH (1988).

Endsley, MR,*Measurement of situation awareness in dynamic systems*,Human Factors, 37, 65-84 (1995).

Hammond, JS, Keeney, RL, and Raiffa, H, *The Hidden Traps in Decision Making,*Harvard Business Review 76, no. 5 (September–October 1998).

Hills, M, *Rehearsing for Reality: Lean Techniques for Reducing Business Risk and Growing Resilience*, International Journal of Emergency Services, April 2015 (forthcoming).

Lakoff, G, *Thinking Points: Communicating Our American Values and Vision,* Farrar, Straus and Giroux, USA(2006).

Lewis, JA, *Cybersecurity and Critical Infrastructure Protection*, Center for Strategic and International Studies (2006), available at: http://cip.management.dal.ca/publications/Cybersecurity%20and%20Critical%20Infrastructure%20Protection.pdfaccessed on 12 March 2015.

Lewis, D, *Addressing the Insider Threat in A Contentious Industry* (working title), MBA Dissertation, Northampton Business School, University of Northampton(forthcoming) April 2015.

MacGillivray, BH, *Fast and Frugal Crisis Management: An Analysis of rule based judgment and choice during water contamination events*, Journal of Business Research, 67, pp. 1717-11724: (2014).

Mcfarlane, P, and Mahajan, R, (personal communication) March 2015.

Moore, T (personal communication) March 2015.

IET, *Resilience and Cyber Security of Technology in the Built Environment*(2013), available at: http://www.cpni.gov.uk/documents/publications/2013/2013063-resilience_cyber_security_technology_built_environment.pdf?epslanguage=en-gbaccessed on 12 March 2015.

Porter, M, *The Competitive Advantage of Nations (1990)*, Harvard Business Review, available at: https://hbr.org/1990/03/the-competitive-advantage-of-nations accessed on 12 March 2015.

Public Safety Canada Action Plan 2010-2015 for Canada's Cyber Security Strategy (2010), available athttps://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdfaccessed on 12 March 2015.

Robinson and Schroeder (2009), *The Role of Front-LineIdeas in Lean PerformanceImprovement*http://twisummit.com/wp-content/uploads/2015/01/The-Role-of-Front-Line-Ideas-Schroeder-and-Robinson-2009.pdfaccessed on 12 March 2015.

Vauughan, D, *The Dark Side of Organizations: Mistake, Misconduct, and Disaster*, Annual Review of Sociology, Vol. 25: 271-305 (1999).