Editorial

Security Journal (2016) 29, 1–4. doi:10.1057/sj.2015.40; published online 14 December 2015

Human Factors in security: User-centred and socio-technical perspectives

Alex Stedmon[a], Dale Richards[a], Lara Frumkin[b] and Peter Fussey[c]

[a]Human Systems Integration Group, Coventry University, Coventry, UK
[b]University of East London, London, UK
[c]University of Essex, Colchester, UK

Over the last 25 years, security research and knowledge has developed in many ways. There have been increased numbers of taught courses relating to criminology and security, high-impact research being published in dedicated journals and, from that, more guidance and support communicated to corporate and private security practitioners (Fisher and Gill, 2012). Some aspects of security research have been driven by recent trends in radicalisation (for example, al Shabab and Islamic State); high-profile terrorist attacks (such as the Westgate Mall attack in Nairobi and Charlie Hebdo attack in Paris); or the need to secure major events (such as the recent Olympics). However, all these developments have seen a growing emphasis on the need to identify indicators of hostile or criminal intent and safeguard public and crowded spaces against potential attacks. In addition, underlying and enduring issues in security have gained prominence, such as the increasing need to consider civil and ethical concerns and responsibilities of those conducting security, along with a clearer understanding of the social and operational contexts and practices of detecting crime.

Many modern security activities embody the notion of complex socio-technical systems with people seeking to work together and use many different technologies to identify hostile intent and respond to security threats (Fussey, 2013). Quite often the focus is on the security stakeholders and security personnel who operate within specific security environments. However, it is also important to consider the user experience of the general public who may be subjected to security interventions during the course of their everyday activities.

From this perspective the discipline of Human Factors and its focus on user-centred approaches has the power to inform new ways of thinking about security. The applied nature of Human Factors has only recently started to be incorporated into security research by combining aspects of applied psychology, systems design, and user experience approaches within the security domain (Saikayasit *et al*, 2013). In order to tackle hostile intent (in all its guises from low-level criminal behaviours through to large-scale terrorist attacks) and develop a socio-technical perspective for security solutions, Human Factors approaches have sought to integrate empirical research with applied methods and approaches grounded in the practical issues faced by security personnel in the field.

With its focus on user-centred and socio-technical perspectives, the discipline of Human Factors has much to offer this endeavour, including:

- an applied knowledge of psychology that can be applied to analyse suspicious behaviours in different contexts;
- a systems-based approach to consider not only hostile intent but also the groups and wider social networks in which criminals operate;
- methods and techniques to support the development of new initiatives and approaches for detecting criminal activities;
- the wider integration of crime prevention into security training, policy and underlying ethical debates surrounding public surveillance; and
- the development of predictive security initiatives through pre-emptive actions (for example, predicting and modelling crime/hostile intent hot-spots through proactive placement of CCTV or predictive and problem-orientated policing).

Given the remit of the *Security Journal*, the guest editors invited authors representing a number of disciplines, including ergonomics/human factors, psychology, criminology, sociology, political science, engineering and computer science, to contribute their knowledge to this area. This special issue

includes six papers that present a mixture of academic and practitioner papers from around the world. Across three themes (systems and organisational security; radicalisation and activism; and security in transport), they all take 'Human Factors in security' as their focus but interpret and translate the issues across highly original and innovative areas, including social theory, nuclear safety and security, the role of families in radicalisation, single-issue bomb attacks, perceptions of vulnerability and operator vigilance.

The first two papers (Fischbacher-Smith and Healey) embrace a systems view of security as the central domain of security ergonomics (Fischbacher-Smith) and for nuclear safety and security (Healey). With reference to recent terrorist attacks and post-Snowden revelations around domestic surveillance and intelligence, Fischbacher-Smith's paper outlines the need to improve the information flows in response to a constantly evolving and more complex threat matrix in order to deal with increasingly challenging task demands. Fischbacher-Smith considers a series of questions about the design of security organisations and their function, within a wider systems context where changes in the environment require corresponding changes in the core processes and functions of a security organisation. When organisations often see security as a 'bolt-on' function to existing activities they will invariably fail to capture the wider strategic dynamics of threat–response interactions and, more significantly, the role that other organisational activities can play in shaping that process.

Healey continues with an organisational perspective by considering aspects of insider threats to both nuclear safety and nuclear security. Civil nuclear organisations must provide evidence for the resilience of their systems to various threats from humans. Some threats are internal and involve human failure, in terms of error or procedural violation. Other threats are more sinister, and involve grievance, malice and criminal intent. Healey argues that safety deals predominantly with internal threat of human failure, whereas security deals predominantly with external threats. However, different threats may share attributes and, if divergent functions do not address convergent threats, this may weaken safety and security defences. As a result, Human Factors provides insights into developing a holistic approach for nuclear risk management.

The following two papers (Spalek, and Lemanski and Wilson) consider factors associated with radicalisation (Spalek) and single-issue bombings (Lemanski and Wilson). Spalek offers an innovative discussion surrounding the role of families in radicalisation, de-radicalisation and counter-radicalisation by exploring links between research, policy and practice. Spalek argues that there are many similarities between the issues identified within the research literature and those highlighted in policy and practice contexts. Both view families as potential propagators of radicalisation while also potentially being sources of protection and rehabilitation. Spalek observes that a focus on families may detract attention away from the wider socio-political factors and may even inadvertently lead to the creation and perpetuation of 'suspect communities'. Families can potentially provide a supportive environment for de-radicalisation and counter-radicalisation, safeguards around human rights, information exchange, and child protection must firmly be in place.

Against a backdrop of the wealth of research conducted on global terrorism over recent years, the paper by Lemanski and Wilson explores single-issue terrorism and conducts a highly original analysis of targeting strategies employed by these groups. Lemanski and Wilson analyse 247 bomb attacks carried out by violent animal rights and anti-abortion extremists worldwide between 1978 and 2008. Using non-metric multidimensional scaling the empirical data are used to construct a model of targeting behaviour that identifies four modes of attack: two of which are primarily designed to cause economic damage or fear, and two of which are potentially lethal to the target occupants. Lemanski and Wilson used the model to compare the tactics of extremists associated with the two different causes and the implications for developing preventative measures.

The final two papers (Hirsch, Kirrilly, Blewett and Every, and Tripathi and Borrion) highlight transport security with a focus on rail applications with an ethnographic study of commuter vulnerability (Hirsh *et al*) and a simulator study investigating train driver vigilance (Tripathis and Borrion). Hirsch *et al* conducted unprecedented field research in India focusing on the most densely crowded trains in the world that have been the target of terrorist attacks in the past. Hirch, in particular, went to Mumbai to interview commuters in order to attempt to redress the lack of research in this area. While a number of government and policy publications analyse threats to passenger security, there has been little effort to understand the impact of hostile intent on the individuals who form the crowd. This user-centred investigation provides insights into day-to-day passenger perceptions of risk and security in

Mumbai (including socio-criminal risks of pickpocketing, molestation and the design-associated risk of falling from the moving train). In addition, it provides an understanding of the legacy of previous attacks on those who use the train service as their 'lifeline' to the city within wider politically motivated risks of terrorism.

Tripathi and Borrion close the special issue with a more traditional approach of a simulation experiment to investigate train driver vigilance for unattended or suspicious baggage. With many transport organisations regarding their employees as important contributors to their security strategies, it is important to examine and understand the socio-technical interactions between service providers, organisational procedures and the systemic security tasks. Tripathi and Borrion determine whether train punctuality goals have an effect on the performance of security procedures. They conducted an experiment on a metropolitan rail system driving simulator to test whether train drivers 'take shortcuts' in the performance of security procedures when they manipulated train arrival punctuality target. Their results indicate that there is a conflict not only between service and security goals, but also between safety and security goals. These findings provide a basis for understanding human behaviour within the wider socio-technical security system and relates back to the earlier papers in this issue of a systems view of security as the central domain of security ergonomics.

Together, these papers represent the forefront of their research areas and bring together topics from a diverse range of disciplines and world-leading research groups to produce a highly original publication. This research contributes to the wider understanding of user-centred and socio-technical perspectives to produce an innovative and informative publication that illustrates the importance of multi-disciplinary discussions in order to facilitate inclusive and ethical strategies, policies and interventions.

References

Fisher, B.S. and Gill, M. (2012) Editor's introduction. Security Journal 25(3): 187–188. | Article |
Fussey, P. (2013) Contested topologies of UK counter-terrorist surveillance: The rise and fall of project champion. Critical Studies on Terrorism 6(3): 351–370. | Article |
Saikayasit, R., Stedmon, A.W. and Lawson, G. (2013) User requirements elicitation in security and counter-terrorism: A human factors approach. Journal of Police and Criminal Psychology 28(2): 162–170. | Article |