Neuroscience perspectives on security

Elena Rusconi[1,2,3]*, Kenneth C. Scott-Brown[2] and Andrea Szymkowiak[4]

[1] Department of Security and Crime Science, University College London, London, UK
[2] Division of Psychology, Abertay University, Dundee, UK
[3] Department of Neurosciences, University of Parma, Parma, Italy
[4] School of Science, Engineering and Technology, Abertay University, Dundee, UK
*Correspondence: elena.rusconi@gmail.com

Security issues have been under the spotlight on a daily basis since the 9/11 terrorist attacks to the Twin Towers, which—aired on live TV—were witnessed by millions of people around the globe. This has been accompanied by the increased availability (and leakage) of security information on the Internet, the increase in public awareness over related issues, and the surge of ethical debates on the possible ethical and legal consequences of "security states"; security has taken priority in political agendas, academic debates, and research funding—the security industry is thriving. Against this background, more and more academics are exploring ways to contribute to the debate, and to inform and influence security decision making. This is both a challenging and a rewarding enterprise and neuroscience promises game-changing innovations.

Security science however is a multidisciplinary field, where physics and engineering, computer science and biology, psychology and medicine, pharmacology and neuroscience, philosophy and jurisprudence, sociology and ethology can all bring valuable contributions to the table. Accordingly, in this Research Topic we have hosted relevant contributions from neuroscience and psychology experts but also dipped into other disciplines such as engineering, physics, computer science, crime science, jurisprudence, and sociology of science. We would like to thank all of the authors and the reviewers for their excellent contributions and their effort in spanning disciplinary boundaries. It is not easy to strike the right balance between expertise and accessibility, to explore a little further outside of our comfort niche and convey meaning to a multifaceted type of readership, such as the one that can be reached via open access and via Frontiers in Human Neuroscience in particular. We hope that our Research Topic will provide a useful contribution to the dialog among disciplines on security-related issues and also a successful example of how the—often artificial—disciplinary boundaries can be challenged.

Almost every aspect of security is inextricably connected with technology. One of the aspects where accelerated advancements have been witnessed in recent years is the incorporation of psychological and physiological measures via new technologies. Reviews of the area of biometrics, traditionally described as the identification of individuals (or their emotional states) using physiological and behavioral characteristics, such as finger prints, iris or retinal patterns, facial features, handwriting or typing on a keyboard (see Ahmad et al., 2013), to name but a few,

and the uses of sophisticated imaging techniques, such as fMRI to detect indicators of deception (see Rusconi and Mitchener-Nissen, 2013; Vartanian et al., 2013), provide two representative examples of this. The ethical and legal aspects of the use of such technologies are widespread. One the one hand, the data gathered with such technology are challenging to process and interpret, so this bears the question as to how clearly experts can present their evidence to a jury in the context of criminal justice systems; on the other hand, findings based on the use of the technology are still far from being fully reliable, research based on laboratory experiments restricts the ecological validity of such measures, and the complexity and sensitivity of the technology makes it difficult to run trials outside the laboratory or even envisage real-world applications. Another question pertains to how transparent individuals and their internal (e.g., emotional, intentional, deceptive, etc.) states can ever be made, even with a fine-grained analysis of human behavior or characteristics, as individuals become aware of advancements in technologies to assess these. Drawing on the concept of measures and countermeasures—can human suspicious behavior and intent be camouflaged so well it is not traceable by the latest neuroscientific detection systems? It is not yet clear to which extent the sophistication of technology and human perception to assess human mental and behavioral activity is juxtaposed with the sophistication of individuals to evade these security measures. Further, fully successful detection systems would have human rights, policy making and social acceptance implications, a critical issue that has been clearly recognized (see Mitchener-Nissen, 2013; Rusconi and Mitchener-Nissen, 2013).

While the above methods investigate physiological or behavioral indices with technological means and algorithms, the use of human operators during incident or threat detection is still irreplaceable and critical to the security discourse (see Howard et al., 2013; Mendes et al., 2013; Stainer et al., 2013). This bears the question on how secure we actually are as both technology and humans are fallible in their decision making. It is, however, generally assumed that the output of visualization techniques such as CCTV and transmission x-rays can be appropriately assessed by trained individuals. CCTV operators are presented with large volumes of constantly updating visual information, and the navigation through this temporal and spatial data feed is very demanding. In transmission x-rays, the difficulty of complex

image interpretation lies mostly in the superposition of several two-dimensional projections and the unusual views by which objects are seen in static images. To gather information about human performance in security image interpretation, diametrically opposite approaches can be adopted—from a classical hypothesis-driven experimental method to an *in situ* observational method reminiscent of a cognitive-ethological approach (Howard et al., 2013; Stainer et al., 2013). While technological improvements are being pursued to increase the efficiency of the screening process from an engineering and physics standpoint, these efforts may be hindered by the intrinsic limitations of the human visual perception system (see Mendes et al., 2013). Notably, to the extent that decisions are made by people, the assessment of potentially dangerous situations in a social environment is subjected to the limitations of the cognitive system that can be swayed or driven by appearances, biases, and previous experience (see Watkins, 2013; Woody and Szechtman, 2013). Of course, the same constraints will also apply to the decisions made by those individuals who actively engage in criminal activities (i.e., those who create breaches in security rather than help maintain it)—an awareness that seems yet to have been fully incorporated in evidence-based crime science (Bouhana, 2013).

Brain manipulation techniques such as Transcranial Magnetic Stimulation and transcranial Direct Current Stimulation may help overcome some of the intrinsic limitations of human security operators with their potential to augment human performance in a range of tasks (Levasseur-Moreau et al., 2013; Parasuraman and Galster, 2013). Although the state of the art may not be mature enough to allow for direct translations into the security field, it is of paramount importance that neuroscientists engage as early as possible with professionals from other disciplines to formulate critical appraisals of the larger-picture implications of any of the envisaged uses (Brunelin et al., 2013; Sehm and Ragert's, 2013). Arguably, rather than hinder or slow down scientific progress, these early multidisciplinary appraisals and interactions will help secure more public support and more resources for neuroscience research.

REFERENCES

Ahmad, N., Szymkowiak, A., and Campbell, P. (2013). Keystroke dynamics in the pre-touchscreen era. *Front. Hum. Neurosci.* 7:835. doi: 10.3389/fnhum.2013.00835

Bouhana, N. (2013). The reasoning criminal vs. Homer Simpson: conceptual challenges for crime science. *Front. Hum. Neurosci.* 7:682. doi: 10.3389/fnhum.2013.00682

Brunelin, J., Levasseur-Moreau, J., and Fecteau, S. (2013). Is it ethical and safe to use non-invasive brain stimulation as a cognitive and motor enhancer device for military services? A reply to Sehm and Ragert (2013). *Front. Hum. Neurosci.* 7:874. doi: 10.3389/fnhum.2013.00874

Howard, C. J., Troscianko, T., Gilchrist, I. D., Behera, A., and Hogg, D. C. (2013). Suspiciousness perception in dynamic scenes: a comparison of CCTV operators and novices. *Front. Hum. Neurosci.* 7:441. doi: 10.3389/fnhum.2013.00441

Levasseur-Moreau, J., Brunelin, J., and Fecteau, S. (2013). Non-invasive brain stimulation can induce paradoxical facilitation. Are these neuroenhancements transferable and meaningful to security services? *Front. Hum. Neurosci.* 7:449. doi: 10.3389/fnhum.2013.00449

Mendes, M., Schwaninger, A., and Michel, S. (2013). Can laptops be left inside passenger bags if motion imaging is used in X-ray security screening? *Front. Hum. Neurosci.* 7:654. doi: 10.3389/fnhum.2013.00654

Mitchener-Nissen, T. (2013). Addressing social resistance in emerging security technologies. *Front. Hum. Neurosci.* 7:483. doi: 10.3389/fnhum.2013.00483

Parasuraman, R., and Galster, S. (2013). Sensing, assessing, and augmenting threat detection: behavioral, neuroimaging, and brain stimulation evidence for the critical role of attention. *Front. Hum. Neurosci.* 7:273. doi: 10.3389/fnhum.2013.00273

Rusconi, E., and Mitchener-Nissen, T. (2013). Prospects of functional magnetic resonance imaging as lie detector. *Front. Hum. Neurosci.* 7:594. doi: 10.3389/fnhum.2013.00594

Sehm, B., and Ragert, P. (2013). Why non-invasive brain stimulation should not be used in military and security services. *Front. Hum. Neurosci.* 7:553. doi: 10.3389/fnhum.2013.00553

Stainer, M. J., Scott-Brown, K. C., and Tatler, B. (2013). Looking for trouble: a description of oculomotor search strategies during live CCTV operation. *Front. Hum. Neurosci.* 7:615. doi: 10.3389/fnhum.2013.00615

Vartanian, O., Kwantes, P., Mandel, D. R., Bouak, F., Nakashima, A., Smith, I., et al. (2013). Right inferior frontal gyrus activation as a neural marker of successful lying. *Front. Hum. Neurosci.* 7:616. doi: 10.3389/fnhum.2013.00616

Watkins, C. D. (2013). Cues derived from facial appearance in security-related contexts: a biological and socio-cognitive framework. *Front. Hum. Neurosci.* 7:204. doi: 10.3389/fnhum.2013.00204

Woody, E. Z., and Szechtman, H. (2013). A biological security motivation system for potential threats: are there implications for policy-making? *Front. Hum. Neurosci.* 7:556. doi: 10.3389/fnhum.2013.00556