Open Access Journal of Forensic Psychology

http://www.forensicpsychologyunbound.ws/ – 2009. 1: 1-4

A Call for Evidence-Based Security Tools

Ewout H. Meijer, Faculty of Psychology and Neuroscience, Maastricht University, Maastricht, The Netherlands. Email: eh.meijer@maastrichtuniversity.nl. Bruno Verschuere, Department of Psychology, Ghent University, Ghent, Belgium. Aldert Vrij, Psychology Department, University of Portsmouth, Portsmouth, UK. Harald Merckelbach, Faculty of Psychology and Neuroscience, Maastricht University, Maastricht, The Netherlands. Fren Smulders, Faculty of Psychology and Neuroscience, Maastricht University, Maastricht, The Netherlands. Sharon Leal, Psychology Department, University of Portsmouth, Portsmouth, UK. Gershon Ben-Shakhar, Department of Psychology, The Hebrew University, Jerusalem, Israel. Pär Anders Granhag, Department of Psychology, Göteborg University, Göteborg, Sweden. Matthias Gamer, Department of Systems Neuroscience, University Medical Center Hamburg-Eppendorf, Hamburg, Germany. Nurit Gronau, Department of Education and Psychology, The Open University of Israel, Israel. Gerhard Vossel, Department of Psychology, Johannes Gutenberg University Mainz, Mainz, Germany. Geert Crombez, Department of Psychology, Ghent University, Ghent, Belgium. Sean Spence, School of Medicine and Biomedical Sciences, The University of Sheffield, Sheffield, UK.

Abstract: Since the 2001 attacks on the twin towers, policies on security have changed drastically, bringing about an increased need for tools that allow for the detection of deception. Many of the solutions offered today, however, lack scientific underpinning.

We recommend two important changes to improve the (cost) effectiveness of security policy. To begin with, the emphasis of deception research should shift from technological to behavioural sciences. Secondly, the burden of proof should lie with the manufacturers of the security tools. Governments should not rely on security tools that have not passed scientific scrutiny, and should only employ those methods that have been proven effective. After all, the use of tools that do not work will only get us further from the truth.

Keywords: security policy, lie detection, deception detection, behavioral science, terrorism

Recently, the peer-reviewed journal *The International Journal of Speech, Language and the Law* yanked an article that unfavourably reviewed voice-stress-analysis software. This software analyzes a speaker's voice, and its manufacturer claims that it can be used for truth verification (See the Nemesysco website at www.lva650.com and http://security.nemesysco.com/gk1.html). Examples of its use entail airport screening (Moscow Domodedovo Airport, 2006) and the evaluation of benefits claims by social services ("Lie detector to target claimants," 2007). The decision by the editorial board was prompted after the company manufacturing the software threatened to sue for defamation (Cho, 2009). Such intimidation and censoring of academic discussion is alarming. The real problem, however, lies in governments actually using these technologies.

Since the 2001 attacks on the twin towers, policies on security have changed drastically, bringing about an increased need for tools that allow for the detection of deception. Potential solutions are primarily sought in new methods and technologies. The US Department of Homeland Security funded the development of the *Future Attribute Screening Technology* (FAST; Barrie, A., 2008), a set of sensors that can remotely measure multiple physiological signals. The US Transport and Security Administration introduced *The Cogito*, another device measuring physiological signals, as well as the *Screening Passengers by Observation Technique* (SPOT), where specially trained teams watch travellers for behavioural signs thought to be indicative of deception (Karp & Meckler, 2006). Meanwhile, the US Defence Academy for Credibility Assessment issued *the Preliminary Credibility Assessment Screening System* (PCASS), yet another device measuring physiological signals, to its soldiers in Afghanistan (Dedman, 2008). Non-US examples of widely used deception detection techniques include the use of the *voice stress analysis* software by British authorities (Cho, 2009), and *Scientific Content Analysis* (SCAN) as one of the worlds most widely used methods to detect deception from written statements (Vrij, 2008). Besides well-chosen acronyms, these methods have one thing in common: They all lack scientific underpinning. None of them is supported by research published in peer-reviewed journals.

In absence of systematic research, users will base their evaluation on data generated by field use. Because people tend to follow heuristics rather than the rules of probability theory, perceived effectiveness can substantially differ from true effectiveness (Tversky & Kahneman, 1973). For example, one well-known problem associated with field studies is that of selective feedback. Investigative authorities are unlikely to receive feedback from liars who are erroneously considered truthful. They will occasionally receive feedback when correctly detecting deception, for example through confessions (Patrick & Iacono, 1991; Vrij, 2008). The perceived effectiveness that follows from this can be further reinforced through confirmation bias: Evidence confirming one's preconception is weighted more heavily than evidence contradicting it (Lord, Ross, & Lepper, 1979). As a result, even techniques that perform at chance level may be perceived as highly effective (Iacono, 1991). This unwarranted confidence can have profound effects on citizens' safety and civil liberty: Criminals may escape detection while innocents may be falsely accused. The Innocence Project (Unvalidated or improper science, no date) demonstrates that unvalidated or improper forensic science can indeed lead to wrongful convictions (see also Saks & Koehler, 2005).

We recommend two important changes to improve the (cost) effectiveness of security policy. To begin with, the emphasis of deception research should shift from technological to behavioural sciences. It is the behavioural sciences that can provide insight into the psychological factors underlying deception. For example, many of the methods described above rely on the assumption that deception is accompanied by some kind of heightened emotional arousal. The robustness of this link between deception and emotional arousal, however, has been criticized in the scientific literature for decades. Consequently, it is not the reliable registration of stress that is cumbersome; it is the relationship between stress and deception that is a problematic starting point (Lykken, 1998; National Research Council, 2003; Vrij, Fisher, Mann, & Leal, 2006). This key problem is addressed by the behavioural sciences, and not by technology.

Secondly, the burden of proof should lie with the manufacturers of the security tools. Currently, the evidence for many of these tools relies almost exclusively upon testimonials or non-disclosed research performed by the manufacturers themselves. This stands in sharp contrast to scientific practice and the recommendation of the US National Research Council. This council— distinguished scholars—concluded that research directed at methods for detection and deterring major security threats should be "*conducted and reviewed openly in the manner of other scientific research. Classified and restricted research should be limited only to matters of identifiable national security*" (National Research Council, 2003, p. 230; see also Bhattacharjee, 2006).

The government's task of protecting her citizens comes with responsibilities. One of these responsibilities entails that decisions about matters with significant potential social or personal implications are based on informed quantitative reasoning (Smith, 1996). Governments should not rely on security tools that have not passed scientific scrutiny, and only employ those methods that have been proven effective. After all, the use of tools that do not work will only get us further from the truth.

Acknowledgements: The authors form The European Consortium of Psychological Research On Deception Detection (EPRODD; www.eprodd.net).

References

Barrie, A. (2008, September 23). Homeland Security detects terrorist threats by reading your mind. Retrieved 7/7/09 from http://www.foxnews.com/story/0,2933,426485,00.html.

Bhattacharjee, Y. (2006). Scientific openness: Should academics self-censor their findings on terrorism? *Science, 312*, 993-994.

Cho, A. (2009). Forensic science: Journal flinches as article on voice analyzer sparks lawsuit threat. *Science, 323*, 863.

Dedman, B. (2008, April 9). New anti-terror weapon: Hand-held lie detector. Retrieved 7/7/09 from http://www.msnbc.msn.com/id/23926278/.

Domodedovo International Airport's clarifications on GK-1 voice profiling technology application. (2006, April 14). Press release retrieved 7/7/09 from http://www.domodedovo.ru/en/main/news/press_rel/?ID=1308.

Iacono, W. G. (1991). Can we determine the accuracy of polygraph tests? In J. R. Jennings, P. K. Ackles & M. G. H. Coles (Eds.), *Advances in Psychophysiology* (Vol. 4, pp. 201-207). London: Jessica Kingsley Publishers.

Karp, J., & Meckler, L. (2006). Which travelers have 'hostile intent'? Biomedic device may have the answer*. The Wall Street Journal,* p. B1.

Lie detector to target claimants. (2007, November 20). *BBC News.* Retrieved 7/7/09 from http://news.bbc.co.uk/2/hi/uk_news/7102920.stm.

Lord, C. G., Ross, L., & Lepper, M. R. (1979). Biased assimilation and attitude polarization: The effects of prior theories on subsequently considered evidence. *Journal of Personality and Social Psychology, 37*, 2098-2109.

Lykken, D. T. (1998). *A tremor in the blood*. New York: Plenum Press.

National Research Council. (2003). *The polygraph and lie detection. Committee to review the scientific evidence on the polygraph. Division of behavioral and social sciences and education.* Washington, DC: The National Academic Press. Retrieved 7/7/09 from http://www.nap.edu/openbook.php?record_id=10420&page=212.

Patrick, C. J., & Iacono, W. G. (1991). Validity of the control question polygraph test: The problem of sampling bias. *Journal of Applied Psychology, 76*, 229-238.

Saks, M. J., & Koehler, J. J. (2005). The coming paradigm shift in forensic identification science. *Science, 309*, 892-895.

Smith, A. F. M. (1996). Mad cows and ecstasy: Chance and choice in an evidence-based society. *Journal of the Royal Statistical Society A, 159*, 367-383.

Tversky, A., & Kahneman, D. (1973). *Judgment under uncertainty: Heuristics and biases*. Oxford England: Oregon Research Inst., Vol. 13.

Unvalidated or improper science (no date). Retrieved 7/7/09 from http://www.innocenceproject.org/understand/Unreliable-Limited-Science.php.

Vrij, A. (2008). *Detecting lies and deceit. Pitfalls and opportunities*. Chichester: Wiley.

Vrij, A., Fisher, R., Mann, S., & Leal, S. (2006). Detecting deception by manipulating cognitive load. *Trends in Cognitive Sciences, 10*, 141-142.