

5-3-2002

Breaches of Homeland Security: Facile Conclusions

Editor

Follow this and additional works at: <https://commons.erau.edu/ibpp>

 Part of the [American Politics Commons](#), [Defense and Security Studies Commons](#), [Other Political Science Commons](#), [Other Psychology Commons](#), and the [Terrorism Studies Commons](#)

Recommended Citation

Editor (2002) "Breaches of Homeland Security: Facile Conclusions," *International Bulletin of Political Psychology*: Vol. 12 : Iss. 16 , Article 1.

Available at: <https://commons.erau.edu/ibpp/vol12/iss16/1>

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in International Bulletin of Political Psychology by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu, wolfe309@erau.edu.

International Bulletin of Political Psychology

Title: Breaches of Homeland Security: Facile Conclusions

Author: Editor

Volume: 12

Issue: 16

Date: 2002-05-03

Keywords: Homeland Security, Security Personnel, Security Studies

Abstract: This article discusses homeland security breaches involving the United States General Accounting Office's Office of Special Investigations.

Yet another in a long line of revelations about homeland security breaches involves the United States General Accounting Office's Office of Special Investigations (OSI). Undercover investigators for the OSI were able to violate the security of four federal government buildings through the use of forged identity badges and persuasive verbal and nonverbal presentations. The investigators were able to obtain after-hours access codes and were allowed to roam through the buildings and introduce objects that could have been or have masked weapons or explosives. But before jumping on the bandwagon of being shocked at such egregious security incompetence, one might pause to consider the phenomenology of security personnel.

It might well be that the undercover investigators were posing as individuals less likely to pose a security threat based on the assumed social attributions and spontaneous profiling of the security personnel. That is, the undercover investigators intentionally may not have "looked like" significant security threats, and, therefore, the security personnel let them pass through security. As a matter of fact, the undercover investigators "looked like" security personnel, and, therefore, the actual security personnel let them pass around security as well. In fact, the undercover investigators were actual security personnel with no malicious intent against federal buildings, and, therefore, the non-undercover security personnel were making security-correct decisions.

One might argue that the non-undercover security personnel's job was not to make security-correct decisions but to practice "good security" through complying with security procedures possibly lacking high validity associated with security-correct decisions. Herein, we see some of the absurdities of traditional security psychology. Rigid adherence to a formal, standard procedure may be far divorced from the intent of the procedure in so far as that intent is to engender security-correct decisions--as opposed to gainful employment for a security industry or to reassurance of the general public. Would the non-undercover security personnel have been commended for letting terrorist-looking individuals (according to the personnel's own attributions and spontaneous profiling) pass through and around security if the right badges and other security paraphernalia and behaviors had been manifested? If the answer to the latter question is in the affirmative, terrorist or other security threats would only have to successfully emulate official images of individuals who are not security threats--an emulation facilitated by requiring rigid adherence of security personnel to a formal, standard operating procedure. Successful emulation would ensure successful security tragedy.

So should the security personnel be punished for making the correct "real" security decision? Should such punishment serve the foundation of homeland security and defense?

This brief analysis of a common public event is not intended to belittle security program research, development, implementation, and evaluation, but only to demonstrate the complexity and challenge of one of history's oldest professions. (See Firestone, D. May 1, 2002). Federal team breaches security in 4

International Bulletin of Political Psychology

buildings. The New York Times, p. A16; Garwood, A. (1999). Psychic security: Its origins, development and disruption. *British Journal of Psychotherapy*, 15, 358-367; Gordon, C., & Arian, A. (2001). Threat and decision making. *Journal of Conflict Resolution*, 45, 196-215; Harden, J. (2000). There's no place like home: The public/private distinction in children's theorizing of risk and safety. *Childhood: A Global Journal of Child Research*, 7, 43-59.) (Keywords: Homeland Security, Security Personnel, Security Studies.)