EMBRY-RIDDLE Aeronautical University
SCHOLARLY COMMONS

International Bulletin of Political Psychology

Volume 3 | Issue 13

Article 3

10-24-1997

Trends. Political Psychology Commentary on the United States' President's Commission on Critical Infrastructure Protection Summary Report

IBPP Editor
bloomr@erau.edu

International Bulletin of Political Psychology

Title: Trends. Political Psychology Commentary on the United States' President's Commission on Critical Infrastructure Protection Summary Report
Author: Editor
Volume: 3
Issue: 13
Date: 1997-10-24
Keywords: Critical Infrastructure, Cyber, Vulnerability, Security, Threat Assessment

The PCCIP summary report released on October 22 in Washington, DC provides at least two overarching conclusions. (1) US "security, economy, way of life, and perhaps even survival, are now dependent on the interrelated trio of electrical energy, communications, and computers" (p. 4). (2) "vulnerabilities (to this trio) are increasing steadily while the costs associated with an effective attack continue to drop" (p. 7). The report also includes a number of security-related statements with significant political psychology import.

(1) "The cyber dimension promotes...blurring traditional boundaries and jurisdictions...National defense is not just about government anymore, and economic security is not just about business...The critical infrastructures are central to our national defense...and we must lay the foundations for...future security on a new form of cooperation between the private sector and the federal government" (p. 1). These statements highlight the import of psychological processes affecting how people conceptualize and categorize--especially those processes related to cognitive rigidity and flexibility. These processes directly affect how policy is developed, evaluated, and implemented. No wonder the report concludes that "New Thinking is Required" (p. 6).

(2) The report's section on "Increasing Vulnerabilities" (p. 4) illustrates the threat of dual usage materials, technology, and knowledge. This section highlights the import of functional fixedness--as its intensity increases among those charged with US security, so does the security challenge. The section also illustrates the sine qua non that critical infrastructure protection must involve thinking from a systems perspective. Unfortunately this perspective often is lost in the deliberative political process of policy and legislative development or is rendered inconsequential by the piece-meal, give-and-take of political horse-trading.

(3) The reports' sections on “A Wide Spectrum of Threats” (pp. 4-6) illustrates the importance of viable personnel security and training programs covering those who work with critical infrastructures. The report does not deal with the usual problems of base rate of problematic intrapsychic processes and behaviors, false positive and false negative rates of indicators, and the cost and practicality of program development and implementation that too often turn good ideas into toothless, ineffectual, even damaging procedures.

(4) The report's "Lack of Awareness" (p. 6) section highlights the need for effective public education programs that not only modify cognitions but also reinforce linkages between these cognitions and compatible security-related behaviors. Relevant psychological theories and experimental data will be necessary to support the report's recommendation for "A Broad Program of Awareness and Education" (p. 8).

(5) The report's "No National Focus" (p. 6) section states that the "infrastructures are so varied, and form such a large part of this nation's economic activity, that no one person or organization can be in charge." This statement highlights the challenge to the field of organizational psychology in fostering

ongoing monitoring and feedback procedures. Another organizational psychology challenge is to help provide procedures to resolve initiatives and philosophical orientations in conflict. For example, the report supports encryption as an impediment to infrastructural threat but does not resolve the vulnerability to such threat posed by a national key recovery system advocated by the Federal Bureau of Investigation--as opposed to a system or systems facilitating data retrieval if keys were lost by their owners. As well, the report ignores the many irrational, illogical, and emotional phenomena--conscious and unconscious--that affect organizational structures, functioning, processes, and mission.

(6) The report's section on "Infrastructure Protection through Industry Cooperation and Information Sharing" recommends variants of risk management procedures that could surely benefit from psychological knowledge on risk perception and the many variables affecting such perception.

The report rightly concludes that "We do not so much offer solutions as directions" (p. 10). However, one does not need a political psychologist to know that the devil is in the details. (See Report Summary: The President’s Commission on Critical Infrastructure Protection, http://www.pccip.gov/summary.html.)