EMBRY-RIDDLE Aeronautical University
SCHOLARLY COMMONS

International Bulletin of Political Psychology

Volume 13 | Issue 3

Article 3

8-23-2002

# Special Article: Recommendations for Optimal Personnel Security in the Cyberworld

Editor

Recommended Citation

Editor (2002) "Special Article: Recommendations for Optimal Personnel Security in the Cyberworld," *International Bulletin of Political Psychology*: Vol. 13 : Iss. 3 , Article 3.
Available at: https://commons.erau.edu/ibpp/vol13/iss3/3

International Bulletin of Political Psychology

Title: Special Article: Recommendations for Optimal Personnel Security in the Cyberworld
Author: Editor
Volume: 13
Issue: 3
Date: 2002-08-23
Keywords: Espionage, Personality, Personnel Security, Sabotage, Terrorism

Abstract. This article considers the social construction of recommendations for personnel security in the context of a global cyberworld.

Even after an intensive exploration of human personality and the essence of personnel security, one still must be ready to accept the notion that recommendations for optimal personnel security contains the seeds of its own self-contradiction.

Part of the problem stems from the context of an ever-changing world within which there are ever-changing people. Even if one could stop the ever-changing aspects of world and people for an instant and accurately embrace that essential moment so as to constitute personnel security recommendations, those recommendations would be but a fleeting Truth that would dissipate even as language describing that Truth were being for the first time recorded for the putative benefit of others.

Part of the problem stems from the basic stance of alienation that persons as personnel necessarily experience within any organization or social context. The assumption that one could conquer or render impotent through some sort of personnel security program the basic psychological and social contradictions of life or intrinsic, tragic elements of some non-verbal and massive Untruth that looms behind what is traditionally conceived of as language may the essence of hubris that all but invites the problematic behaviors of sabotage, espionage, and terrorism that have concerned us.

It may well be that the quests for personnel security recommendations and for effecting such recommendations are only a vehicle to blame and exploit persons as personnel for being persons. Or, perhaps, these quests exemplify the false consciousness of personnel security authorities whose very sincerity in their efforts display their own misunderstanding psychological and social forces impinging and impacting on themselves. Nevertheless, let's look at a few common personnel security recommendations for what they might offer and how they might be contemplated.

Recommendation 1. Trust No One. This recommendation might seem at odds with the rationale of many personnel security programs that seek to effect trust in each person, between and among people, or among all people towards some external object-e.g., God, the organization, the organizational motto-that is insistently idealized so as to be identified, internalized, incorporated, introjected, or complied with. In fact, one might argue that by trusting no one and communicating this personnel security stance, one only constructs expectations and self-fulfilling prophecies leading to organizational security self-constructed wounds.

Of course, a counter to this argument is that the operationalized perspective of trusting no one activates reactance-a motivating tendency to act contrary to expectations. In such a case, publicizing and operating on a non-trusting stance would be expected to induce trustworthy behavior to spite the organization, as opposed to protect it. The problem here is that such contrariness then becomes a self-fulfilling prophecy and that reactance then leads to the contrariness of acting contrary to the new-self-fulfilling prophecy-i.e., acting against the interests of organizational security-in a never-ending dialectic that oscillates back and forth from trustworthy to nontrustworthy behavior as opposed to progressing towards some ultimate security Nirvana.

The fact remains that given the personality perspective that persons as personnel present an a priori security vulnerability, one must assume that all people-regardless of selection process-are security threats. All people will think, feel, be motivated, and act in a manner that is not in the best interest of the organization whose security is the primary concern-even if they think that they do have this primary concern.

As some sort of saving grace, one should also note that people as personnel certainly differ within the organization in terms of quantity and quality of security risk. And given the omnipresent security reality of finite security resources, one does not have the choice of treating all people equally and at adequate depth. So, in essence, while no one should be trusted, some people should be distrusted more than others, and all people should be distrusted differently than others. This observation leads to the next recommendation.

Recommendation 2. Distrust Everyone Differently. As alluded to by many personality theorists and implied by still others who are not involved in such alluding, the construct of personality suggests that all people are like all other people in some ways, like some other people in some ways, and like no other people in some ways. All people also have unique ways of being like some other people in terms of all possible combinations of ways and other people. As well, all people have unique ways of manifesting combinations of being like all, some, and no others.

Concrete examples of these abstractions can be identified in the self-reports and accompanying investigative analyses related to why people as personnel engage in sabotage, espionage, and terrorism. The usual suspects of motivations include money, ideology, some perceived slight at the hands of the organization or some other entity represented by the organization, searches for meaning in and control of one's life, sensation seeking, overcompensation for feelings of inferiority, exploitation and coercion by other people, and engaging in de facto mindlessness-this last characterized by not realizing that the behavior engaged in is problematic and constitutes some combination of sabotage, espionage, and terrorism.

However, although each of these classes of motivation-and others too statistically deviant, unspeakable, or unknown to be mentioned-can be populated by persons as personnel who have engaged in problematic behavior, each person is a unique case. As just one example, each person has a different stance and take on what money means, how much is needed over what schedule, the degree of a sense of entitlement, what will be done with the money, beliefs about money serving as a motivational vehicle for problematic behavior, and so on. As another example, each person may represent a combination of motivations-none of which are sufficient and only some of which may be necessary.

The epistemological Issue for personnel security experts then becomes how does one know what needs to be distrusted in each person as personnel and how can one best monitor what needs to be distrusted. The "same-size-fits- all" approach to personnel security is analogous to the random and mindless security screening of passengers at airports wherein every fifth or ninth person is stopped for additional attention-an approach that does no more than throw in the towel on any putative value of human intelligence unless randomness would actually correspond to the Way of the World. Until such a "surgical strike" or profiling approach can be developed, implemented, and evaluated on a continuous basis founded on the ever-changing world and the people within it, only luck, Fate, and forces beyond human comprehension will be the source of personnel security success.

Recommendation 3. Remember What's Important. Too often, persons as personnel with authority make decisions about the lives of persons as personnel based on "making a point." The "point" may be that persons as personnel with authority must be obeyed; that an organization and its constituents-e.g., the personnel life-is more important than a person's personal life. Or the "point" may be that a policy manual must be followed in some special variant of a very strict constructionist perspective. The point may even be unconscious in that the criterion for making decisions about the lives of persons as personnel (of which the person as personnel with authority is unaware) is the best resolution of unconscious psychodynamic conflict of that person with authority-even as that conflict may have largely precipitated whatever personnel Issue crystallized as crisis and as requiring some sort of decision and action.

From a personnel security perspective, however, what's really important is what will prevent, minimize, or manage problematic behavior and associated noxious consequences. So along with matters of substantive, procedural, and distributive justice comes the security potential not of persons as personnel but of the very security decisions for the organization. This potential should be factored into job assignments, transfers, lay-offs, promotions, awards, firings and latest organizationally constructed and totalitarian-like scandal mongering.

Recommendation 4. Only Protect What Needs To be Protected. Three enemies of personnel security are classification inconsistency, overclassification, and underclassification. (Here, classification can apply to actual security classifications-e.g., Top Secret-classification of information as sensitive or requiring some sort of special access, or classification as to what constitutes a need-to-know.) Inconsistency, overclassification, and underclassification are largely personality-driven in terms of idiosyncratic perceptions of what an organization values as appropriate classification, of unconscious psychodynamic conflict concerning secrecy and power, and of primitive and quantitative aphorisms about more or less being better regarding "good security." These personnel security enemies can result in a disrespect for the rule of law and regulations, lowered motivation for following the letter and the spirit of laws and regulations, and actual decrements in behavioral compliance with laws and regulations.

Conclusion. The upshot of an exploration of optimal security recommendations is that personnel security authorities need to be engaged not in Truth detection but in a never-ending dialogue within themselves, among members of the organization, and the persons and world in which an organization is situated. The ever-expanding cyber context makes this dialogue evermore complex but evermore demanding. Multiple selves, disguised personas, and cyber-produced psychological and social change all contribute to the challenge of personnel security and identifying the remaining robustness of anything that might constitute the timelessness of human psychology and behavior. Such a conclusion may only anger the personnel security authorities of today who long for and demand certainty and consider ambiguity as moral, ethical, and even psychological weakness. However, it is our fate that it is only ambiguity that we can be certain of. (See DiBattista, R.A. (1996). Forecasting sabotage events in the workplace. Public Personnel Management, 25, 41-52; DiBattista, R.A. (1991). Creating new approaches to recognize and deter sabotage. Public Personnel Management, 20, 347-352; Klein, R. L.; Leong, G. B.; & Silva, J. A. (1996). Employee sabotage in the workplace: A biopsychosocial model. Journal of Forensic Sciences, 41, 52-55; Sieh, E.W. (1987). Garment workers: Perceptions of inequity and employee theft. British Journal of Criminology, 27, 174-190; Tucker, J. (1993). Everyday forms of employee resistance.

Sociological Forum, 8, 25-45.) (Keywords: Espionage, Personality, Personnel Security, Sabotage, Terrorism.)