International Bulletin of Political Psychology

Volume 13 | Issue 1 Article 4

8-9-2002

Musings On One Who Got Away: Personnel Security, Counterintelligence, and Edward Lee Howard

IBPP Editor
bloomr@erau.edu

International Bulletin of Political Psychology

Title: Musings On One Who Got Away: Personnel Security, Counterintelligence, and Edward Lee Howard
Author: Editor
Volume: 13
Issue: 1
Date: 2002-08-09
Keywords: Counterintelligence, Espionage, Personnel Security

Abstract. This article describes several concerns with the United States Government's (USG) approach to minimizing betrayal by its personnel who are entrusted with security clearances, special access to sensitive information, and sensitive positions.

It is the author's contention that all personnel security programs bearing on the probability of personnel's problematic behavior are personality-based. Not that they should be, or not necessarily that they have to be, but that they are. That is, signs, symbols, other semiotics, and various combinations and permutations of cognitions, emotions, motivations, and behaviors are the sine qua non of labeling persons as personnel as sources of problematic behavior. Even if historical, situational, and other contextual perspectives also are employed in evaluating personnel, personnel authorities seem to reify the person as opposed to the situation as the ultimate source of betrayal.

Has this approach been successful? Certainly, there have been US citizens and persons contractually supporting USG objectives who betrayed the government or at least tried to (cf. Heuer & Herbig, 2001; Wood and Wiskoff, 1992). Some persons included in this grouping actually might have been double agents who--unbeknownst to the general public and, perhaps, to others--were all along "really" working for the USG but just acting as if they were attempting to betray it. However, it seems as if most of the individuals publicly accused and convicted of charges bearing on the problematic behavior of espionage, as well as sabotage and terrorism, did indeed engage in such behaviors. While it also seems as if the vast preponderance of persons as personnel who are formally trusted by an organization do not engage in significantly problematic behavior, the nature of security and sensitivity suggests that even a very, very small number of personnel who "go bad" may be too bad for the organization-both in terms of commiserating with that organization and in the noxious consequences of the problematic behavior.

One policy source exemplar of personnel security programs within the USG is the United States Government's (USG) Director of Central Intelligence Directive (DCID) 6/4: Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI). The DCID 6/4 is intended to facilitate the adjudication of personnel who may receive or maintain security clearances, special access to sensitive information, or sensitive positions. As this text is being written, a commentary on vulnerabilities inherent in such a personality-based program may be very timely in light of the recent death of Edward Lee Howard (Tavernise, 2002). Howard seems to have defected to the Soviet Union in 1985, apparently after failing a polygraph about petty theft and drug use and after selling sensitive information to Soviet authorities in 1984 (Wise, 1988). With perfect retrospective vision, one would conclude that it might have been more prudent not to have trained Howard and his wife as an intelligence case officer team in sensitive information gathering techniques.

What were the personnel security criteria to which they were held in their initial contacts with the USG Intelligence Community? Although the predecessor to the DCID 6/4, the DCID 1/14, was the operative document at the time, the overlap between the two is extremely significant, and there are similar concerns from a personality and personnel security perspective about both. (All following references are for the DCID 6/4.)

(Introduction, p. 1). The DCID 6/4 is intended "to promote the use of common and consistent standards for government-wide security background investigations." However, identical standards may have radically different meanings for different personnel and vastly different predictive validities for said personnel. Common and consistent standards constitute an ideology with high face validity for the general public but with a highly complex relationship with human psychology for socially sanctioned experts.

(1. a., p. 2). The DCID 6/4 stipulates that the psychology of "cohabitants" of a person being adjudicated for SCI access is personnel security-relevant. However, a "cohabitant" is defined as "a person living in a spouse-like relationship" with the person being adjudicated. Yet, spouses may not have a spouse-like relationship with the adjudicatee, while other cohabitants without a spouse-like relationship with the adjudicatee may have very significant effects on the relevant psychology of the adjudicatee. And the fact of actually living together or not may or may not be germane to relevant personnel security concerns. The same reasoning applies to the construct of "immediate family" referred to on p. 3 of the DCID 6/4 (1. d., p. 3) wherein "immediate family" is defined as the spouse, parents, siblings, children, and cohabitant" of the adjudicatee.

(5. a./5. b., p. 4). The DCID 6/4 stipulates that the adjudicatee and the adjudicatee's immediate family must be US citizens. The assumption here appears to be that one's citizenry has a high correlation with loyalty to the relevant government and nation. However, there are US citizens and non-US citizens who would and would not violate the trust of the USG. One might also argue that in an era of globalization, internationalization, and facilitation of telecommunications and mobility, different people may place more or less significance on their citizenship. Thus, citizenship may not present much of unique predictive value or of unique threat status for an entire adjudicatee population of an organization but only for some subpopulations, not all of whom are obvious or even knowable.

(5. c., p. 4). The DCID 6/4 stipulates that associates of the adjudicatee should not "be subject to physical, mental, or other forms of duress by a foreign power." However, a related security vulnerability would also include duress by a conscious or unconscious sense of affinity for a foreign power that might lead to a rationalization that engaging in an action supporting a foreign power would be concurrently and appropriately supporting the US. Such an example of rationalization-a defense mechanism that is unconscious by definition and is designed to attenuate anxiety associated with consciously expressing something that is extremely psychologically threatening to express-suggests the psychological complexity of believing that personnel security violation may support some combination of both the foreign power and/or the USG. This complexity is even further compounded by addressing the hermeneutic difficulties of any text that has such significant implications for both a collective of persons and any individual person. In fact, these difficulties border on both the Talmudic and the exegetic, depending on one's religious proclivities.

(5. d., p. 4). Perhaps the most essential vulnerability of the DCID 6/4 is its stipulation that the adjudicatee "must be stable; trustworthy, reliable; of excellent character, judgment, and discretion; and of unquestioned loyalty to the United States." Such persons as personnel are exactly the kinds of persons who are most noxious to the security of an organization, once said persons decide to work against it or work against it while believing that they are working for it.

A traditional personnel security assumption is that such persons would rarely ever want to work against their organization or rarely ever work against it while believing that they are working for it. However, there are situations of egregious crisis for the organization or for the organization as perceived by these persons as personnel-situations involving grievous organizational malfeasance-in which stability, reliability, and the like would very likely engender personnel security violations. These situations are characterized by the organization's or some of its representatives', own material viability wrongly subsuming the formally professed goals of that organization and the government and nation of which it is a part. In such situations, it is the mindless or often enough morally and ethically bereft type of personnel who would not engage in such violations.

Another traditional personnel security assumption is that the organization can never engage in such grievous malfeasance or has built-in mechanisms or is associated with relevant external monitoring devices that virtually preclude such malfeasance. Yet it is the sense of grievous malfeasance as perceived by personnel security violators that quite often is a final common behavioral pathway for many violators. Here, malfeasance does not only include illegal financial and political actions but-in the eyes of the violators-organizational decisions not to promote, reward, recognize, or aid to the degree desired and judged appropriate.

As an additional point, one should note that the USG has taken an ambivalent stance on the value of loyalty. Although virtually any USG personnel believes that an absence of loyalty or of adequate loyalty to the USG would automatically bar a person from any federal or federally funded position (cf. Security requirements, 1953), Lewy (1986) has argued that loyalty as a requirement for USG employment has not been used for potential employees who formally will not require access to classified information. The problem here is not only the heterogenous relationship between loyalty and problematic behavior, but also the temporally and cognitively dependent nature of what information merits classification, what pathways constitute access to such information, and how the transmission of seemingly non-sensitive information may have dire consequences in some situations.

(6., pp. 4-5). The DCID 6/4 does allow for exceptions based on "common sense" in that aspects of what are considered valid predictors for personnel security may be knowingly overlooked in specific cases. This exception policy in and of itself is a good one in that it allows for the lack of complete validity between an assumed predictor and security-related behavior and other problematic behavior. However, the assessment excepting the specific case "become(s) a part of the individual's security record." In other words, the adjudicatee-now as personnel-must carry this exception as an albatross throughout a career with the organization. The exception then can become a festering sore for personnel and is likely to be noticed when any organizational decision goes against personnel preferences.

(7. e., p. 6/12. b. (5), p. 10). The DCID 6/4 stipulates that the polygraph can be employed in the adjudication process. However-assuming the need for organizational security is not reified over appropriate scientific standards-one must advocate for a very constrained polygraph employment. The psychophysiology of deception in various interview modes is such that the polygraph should be used to generate hypotheses that can then be supported or not by other types of information. Polygraphic data in and of themselves should not be grounds to make personnel decisions or other decisions bearing on personnel security violation. One can make a strong argument that unfavorable decisions based solely on the polygraph-especially for persons already privy to sensitive information-may harm organizational security much more than whatever harm was feared based such data alone. This last statement is the

case both for persons as personnel who are reactively driven to engage in problematic behavior and who are essentially blameless and innocent but whose significant contributions to USG security are thereby impeded, put on hold, or permanently discontinued.

(9., pp. 7-8/ 12. b. (1), p. 9/Annex C, 2., (e) & (f), p. 2). The DCID 6/4 stipulates that adjudicatees and persons as personnel must "report activities, conduct or employment that could conflict with their ability to protect" information from unauthorized disclosure or counterintelligence threats." There are several problems here. First, personnel security programs cannot be written in an inclusive fashion. Thus, the concerned and loyal person as personnel must guess for many activities what may or may not be problematic. Second, the reinforcement, omission training, and punishment contingencies for organizations-even for those which may deny it or attempt to comply with said denial-is to much more easily treat reporters in a negative than positive fashion. In other words, omission training and punishment will win out over positive or negative reinforcement. This state of affairs leads to most of the guilty and some of the innocent avoiding the reporting requirement. The innocent meeting the requirement will be less likely to do so in the future-assuming these innocent are still with the organization in the future-as organizational pressures to prove a negative (that one hasn't done anything wrong) increase.

(12. a., p. 8). The DCID 6/4 concerns itself with "Issues which bring into question an individual's integrity". Also, DCID 6/4 highlights "activities which indicate character flaw" that is handled as a lack of integrity. However, integrity is a problematic term that may hurt more than help personnel security. Integrity may denote honesty, even as complete honesty most often qualifies one for a hard life, including personal retribution, imprisonment, and incarceration. Integrity may include leading a lifestyle compatible with what is deemed to be a proper way to live one's life by an organizations' highest authorities. Yet the selection for or conforming to the authorities' preferred lifestyles may often enough be orthogonal to an organizations' mission and security. Moreover, making personnel security decisions based on this latter sort of integrity may harm the organizational security more than keeping or throwing these people out of the organization. One way this harm can occur is when shared identification and compliance with a preferred lifestyle is used as a point of departure to gloss over, deny, or otherwise excuse significant security misbehavior. Another can occur when non- identification and non-compliance can lead to driving out those with security excellence.

(Annex B, 3. pp. 1-2). The DCID 6/4 stipulates that a personnel security investigator "should plan and execute each interview so as to obtain the maximum amount of information from a source." However, persons as personnel or persons speaking about persons as personnel or just as persons can use the imparting of voluminous information to avoid imparting relevant and accurate information that might contribute to not selecting or not retaining a person. Thus, the admonition to obtain a maximum amount of information actually can facilitate hiding relevant and accurate information. In fact, non-relevant garrulousness is often enough recommended as an approach to keeping what an adversary wants to know from an adversary.

If instead, the idea is for an investigator to secure all relevant information, the problem then becomes how does one know when all relevant information is obtained-or even when information is relevant as opposed to irrelevant? The enemy of differentiating the relevant from the irrelevant is the seeming face validity of information and a literal interpretation of security manual text.

(Annex B, 4. c. (5), p. 3). The DCID 6/4 stipulates that "If a source provide derogatory information, the investigator should report as fully as possible; (5) Whether the conduct was voluntary or whether there was pressure, coercion, or exploitation leading to the conduct; (and) (6) Whether the Subject has been rehabilitated." However, whether the conduct was voluntary or via pressure/coercing/exploitation should not-by DCID 6/4's logic-have a bearing on the personnel security viability of a person as personnel, because both motivational pathways are contraindicated as antitheses of personnel security. (Another possibility might be unknowingly engaging in activity that can be characterized as derogatory behavior-a possibility that may be addressed through conceptual approaches such as cognitive and mental health but again have no bearing on the consequences of problematic behavior.)

A related Issue is the potential for rehabilitation after engaging in problematic behavior-i.e., engaging in something labeled as derogatory that allegedly has a bearing on engaging in espionage or other problematic behavior such as sabotage and/or terrorism. The problem here is that assessing rehabilitation is an extremely complex and probably unknowable venture in that the situation(s) in which a person as personnel has engaged in problematic behavior may not ever completely return once the person has been identified as having engaged in problematic behavior. On the one hand, this might be interpreted as suggesting that the person has been rehabilitated in the sense that the problematic behavior can no longer appear without its eliciting stimulus. On the other hand, there may be other eliciting stimuli that are unknown to personnel security authorities and even to the person in question that will elicit the problematic behavior.

(Annex C, 2., (b), p. 1). The DCID 6/4 stipulates that "Each case must be judged on its own merits." This stipulation has positive and negative consequences for the selection and retention of person as personnel in the security context. Positively, judging each case on its own merits avoids the response set or ideology that all cases and all fragments of information in all cases must be handled the same-the latter being a prescription for rigid, thoughtless, and mindless determinations of human resource management. Negatively, judging each case on its own merits can be exploited through legal intervention by persons seeking to harm the security of an organization and by persons who believe in the ideology that all cases and all fragments of information in all cases must be handled the same as the only means to avoid legitimate discrimination and harassment suits.

(Annex C, Guideline B., 7., (e)). The DCID 6/4 stipulates that "Conditions that could raise a security concern and may be disqualifying include: (h) a substantial financial interest in a country, or in any foreign owned or operated business that could make the individual vulnerable to foreign influence." However, a trend in business within an era of globalization is to locate headquarters and the venue of incorporation in foreign entities-a trend that could have negative personnel security consequences for many financial contributors to political campaigns and for many corporate authorities seeking influence within a government including access to sensitive information and authorization to engage in sensitive activities.

In all the above, one might sense a tension among the nomothetic, the idiographic, and the idiothetic-respectively, what might apply to people in general, what might apply just to an individual, and what might apply just to an individual based on what applies to people in general. The USG personnel security approach as inferred from the DCID 6/4 is primarily nomothetic regardless of protestations to the contrary. Such an approach has an intrinsic error range when applied to each individual person as personnel being initially selected or re-investigated after selection. In certain lines of work, the error range can be tolerated, because the consequences of making mistakes in evaluating any particular person as personnel may not be especially catastrophic. However, in the world of international and

national security-specifically dealing with cybersecurity-any particular person may well represent a much higher probability of catastrophe if the wrong evaluation is made.

There is a converse Issue as well. As mentioned above, the person as personnel who is wrongly barred from being selected or from continuing on the job may represent a catastrophic loss in unmined talent and achievement for the organization engaged in the barring. A case in point is the legendary Felix Dzerzhinsky-the Bolsheviek and Soviet personnel security and counterintelligence stalwart (The psychology, 1996).

In conclusion, something similar to the aviation security notion of a trusted traveler program might be germane for personnel security selection and re-investigation. Beyond those whom Kenneth Adelman (2002) terms "accomplished Americans," all applicants surviving a check for past felonious behavior and felony criminal convictions would be selected if relevant skill and experience requirements were met. And all personnel would remain in the system if job performance were adequate and felonious behavior and felony convictions avoided. Random counterintelligence screens would still be ongoing, but as Adelman (2002) points out, character assassination and vicious and irrelevant gossip imparted by "jealous job-seekers, bested business competitors, partisan foes, jilted lovers, and ex-spouses" would be minimized. (See Heuer, Jr., R.J., & Herbig, K. (2001). Espionage by the numbers: A statistical overview. Defense Personnel Security Research Center: Monterey, CA; Hibler, N., & Christy, J. (1993). Understanding the computer criminal. Paper presented at the Department of Defense Computer Crime Conference. Monterey, CA; The psychology of counterintelligence: Felix Dzerzhinsky and postmodern dilemma. International Bulletin of Political Psychology, 1(3), http://security.pr.erau.edu; IBPP Leonard, J.W. (July 16, 2002). Remarks at the National Classification Management Society's (NCMS) Annual Training Center. Ft. Worth, TX; Lewy, G. (1986). The federal-security loyalty program. In R. Godson, (Ed.). Intelligence requirements for the 1980s: Domestic intelligence. Lexington, MA: Lexington; Security requirements for government employment, (April 27, 1953). Executive Order 10450; Tavernise, S. (July 23, 2002). Edward Lee Howard, 50, spy who escaped to Soviet haven, is dead. The New York Times, http://www.nytimes.com; Post, J.M. (Undated). The dangerous information systems insider: Psychological perspectives. Manuscript; Wise, D. (1988). The spy who got away. Random House; Wood, S., & Fischer, L.F. (2002). Cleared DOD employees at risk. Report 1. Policy options for removing barriers to seeking help. Defense Personnel security Research Center: Monterey, CA; Wood, S., & Wiskoff, M. (1992). Americans who spied against their country since World War II. Defense Personnel Security Research Center: Monterey, CA.)(Keywords: Counterintelligence, Espionage, Personnel Security.)