FREUDENBURG BEYOND BORDERS: RECREANCY, ATROPHY OF VIGILANCE, BUREAUCRATIC SLIPPAGE, AND THE TRAGEDY OF 9/11

Susan Maret

ABSTRACT

In this chapter, I suggest three conceptual tools developed by William R. Freudenburg and colleagues that characterize the failure of institutions to carry out their duties – recreancy, atrophy of vigilance, and bureaucratic slippage – are of use beyond environmental sociology in the framing of the September 11, 2001 disaster. Using testimony and findings from primary materials such as the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence Joint Inquiry hearings and report (2002, 2004a, 2004b) and the National Commission on Terrorist Attacks Upon the United States (2004) alongside insider accounts, I discuss how Freudenburg's tools have the potential to theorize institutional failures that occur in national security decision making. I also suggest these tools may be of particular

William R. Freudenburg, A Life in Social Research
Research in Social Problems and Public Policy, Volume 21, 201–223
Copyright © 2013 by Emerald Group Publishing Limited
All rights of reproduction in any form reserved
ISSN: 0196-1152/doi:10.1108/S0196-1152(2013)0000021013

interest to the U.S. intelligence community in its own investigation of various types of risk and failures.

Keywords: 9/11 attacks; William R. Freudenburg; House Permanent Select Committee on Intelligence; National Commission on Terrorist Attacks Upon the United States; Senate Select Committee on Intelligence; U.S. intelligence community

INTRODUCTION

Known primarily as an environmental sociologist, William R. Freudenburg's research is informed by critical theory, postructuralism, and institutional ethnography. With their emphasis on power, privilege, legitimation, language, and concern with the construction and limits to knowledge, these schools of thought flow through Bill's work, especially in his analysis of risk (Freudenburg, 1993, 1996a, 1996b, 2001), and call for the "systematic use of social science in risk analysis" (Freudenburg, 1992, p. 3).

As Tom Rudel points out in this volume, during a two decade period, from 1985 and 2005, Bill "created a portfolio of conceptual tools that could be used to analyze the politics of natural resource regulation." During this period of time, Bill *also* created conceptual tools that are essentially tied to risk perception, risk communication, and risk aversion in institutional settings – recreancy, atrophy of vigilance, and bureaucratic slippage – the latter constructed with colleague Robert Gramling.

These tools do not appear to have widely diffused from environmental sociology into the general social science research literature or the security and intelligence studies literature.[1] This is puzzling, especially when one ponders the emphasis on risk assessment in the post-September 11 climate and subsequent recommendations of the Commission on the Prevention of WMD Proliferation and Terrorism's *World at Risk* report (2008), which predicts "it is more likely than not that a weapon of mass destruction will be used in a terrorist attack somewhere in the world by the end of 2013" (p. xv). Post-9/11, the U.S. intelligence community, or IC,[2] is tasked with establishing "uniform policies, approaches, guidelines, and methodologies for integrating Federal infrastructure protection and risk management activities within and across sectors along with metrics and criteria for related programs and activities" (Homeland Security Presidential Directive 7, 2003).[3] Further, it has been suggested that "intelligence itself is a risky means of shifting risks; risky in the sense that its product is often of ambiguous value, and its fragile methods can provoke angry and dangerous responses from their targets" (Warner, 2009, p. 24). Risk, as defined in intelligence settings, is

> 1. The probability that a particular threat will exploit a particular vulnerability of national security that will result in damage to the life, health, property, or the environment. 2. The probability of loss from an attack or adverse incident. It is a function of threat (adversaries' capabilities, intentions, and opportunities) and vulnerability (the inherent susceptibility to attack). Risk may be quantified and expressed in terms such as cost in loss of life, dollars, resources, or programmatic impact. (Goldman, 2011)[4]

To this end, I suggest Bill's conceptual tools (recreancy, atrophy of vigilance, and bureaucratic slippage) have a role to play in theorizing terrorism-related disasters that involve national security decision making. Risk plays an important part in these tools, especially in cases where "the lack of organizational commitment to risk management may be a *predominant* source of *real* risk" (Freudenburg, 1992, p. 12). Within a narrow band of research, I provide background on these tools, and include commentary from hearings, reports, and insider accounts on the September 11 tragedy. These sources indicate failure to detect the attacks are not only complex, but have a basis in past policies and decisions, and involve a system-wide collapse of communication and subsequent policy actions among multiple federal agencies and bodies. In making this association, I suggest that Bill's tools are not only of methodological assistance to researchers in investigating system-wide institutional failure as illustrated by the 9/11 case, but can play a part in the IC's *own* examination of intelligence and warning failures, perhaps even providing a theoretical foundation for "lessons learned" (Johnston, 2005).[5]

CONCEPTUAL TOOLS: RECREANCY, ATROPHY OF VIGILANCE, AND BUREAUCRATIC SLIPPAGE

As ideal types,[6] Bill's recreancy, atrophy of vigilance, and bureaucratic slippage share several elements in common.[7] First, there is a focus on information as "any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual" (Office of Management and Budget, 1996). If we recall Max Weber's (1978) work on the significance of the files to the inner workings of the bureaucracy as "efficient machine" (p. 973). Information takes on supreme importance as a gauge of risk and uncertainty in institutional decision making, and may exist in such abundance that it is difficult for institutions to sift and filter in order to get at "needed information" (Clarke, 2008, p. 97).

Further, as responsibility for decision making is situated within information hives within hives, in the form of agencies, subdepartments, and units replete with formal rules, some secret, some not (e.g., standard operating practices and procedures, forms, directives, classification) there remains an emphasis on data collection, record keeping, and the creation of reports that serve calculation (Weber, 1958, p. 139). Second, Bill's tools share an emphasis on the total institution and their agencies, subdepartments, and units in not "connecting the dots" relative to risk, threats, and/or warnings. Lastly these conceptual tools infer that a diminishment of trust and confidence in an institution's policies and actions can occur through identifiable means.

The first conceptual tool in Bill's theoretical trifecta is *recreancy*. Bill made an interesting choice in selecting this term to convey that "persons entrusted with the operation of systems may have failed to carry out their responsibilities with the necessary vigor" (as quoted in Freudenburg & Jones, 1991, p. 1159), "not getting the job done" (Freudenburg, 1993, p. 916), and "a retrogression or failure to follow through on a duty or a trust" (Freudenburg, 1996a, p. 47). Although Bill drew from etymological roots in his application of recreancy, (the Latin *re-* (back) and *credere*, to entrust), the word was used as early as 1602, and also strongly defined as "apostasy, treachery; mean-spiritedness" (Oxford English Dictionary, 2013). The form *recreant* conveys being "unfaithful to duty or a person" but also "designating a person who admits to having been defeated or overcome; that yields or surrenders; in a condition of surrender or defeat" (Oxford English Dictionary, 2013).[8] All of these definitions capture a failure to follow through and faithfully act on a duty; however, by way of additional meanings such as *defeat and surrender*, recreancy may also suggest an inability to carry out a responsibility through an *overpowering*, and/or *being overwhelmed*, perhaps by way of internal institutional dynamics, outside forces, or both. This meaning will take on greater significance in the next section of my discussion.

Building on Bernard Barber's (1983) research on trust, Bill assigned to recreancy failings in technical competence and fiduciary responsibility, "but the term is also intended to describe cases where the failing is neither a matter of (individual) incompetence nor one of self-interest" (1993, p. 917). Utilizing a "Weberian-institutional perspective," Bill (Freudenburg, 1993) observed that failure to protect the public interest may lead to not only challenges regarding authority or "expert control," but exemptions from public analysis of policies and the information in which they are based. Recreancy therefore also involves a potential reduction in social capital:

> *Credibility* refers to *believability*, not to the broader range of behaviors (and failures to "behave") that constitute a failure to perform specialized duties in an appropriate manner. *Trust* is usually exercised or withheld by those who assess the performance of institutional actors, not by the institutional actors themselves. *Trustworthiness* would come as close as any common word to the meaning that needs to be conveyed, particularly if we think in terms of the two primary considerations in Barber's discussion of trust relationships (1983) – technical competence and fiduciary responsibility. For the interests of the society at large to be properly protected, after all, the relevant specialists and institutions need to be both competent and properly reflective of their responsibilities to the broader collectivity. (Freudenburg, 1993, p. 916)

In formulating the concept of recreancy to describe failings, Bill, much like Weber before him, was acutely aware of the limits of language and need for researchers to create original vocabulary to mirror social phenomena. He argued for "a specialized word if we are to refer to behaviors of institutions or organizations as well as of individuals and, importantly, if the focus of attention is to be on actual behaviors" (1996a, p. 47). Bill (1993) was also attentive to those researchers "who object to the term of recreancy it may be possible to refer instead to institutional failure, although this alternative terminology can convey a meaning that is far less precise" (p. 917). Recreancy then is a useful tool to characterize situations where policies and procedures go awry, and where "the 'responsible' person or organization can prove almost impossible to find" (Freudenburg, 1996a, p. 47). Recreancy is especially useful in examining conditions

> Where a major technological accident does occur – and unfortunately, the question seems to be one of when and where, rather than of whether – disruptions may be created not just by the accidents themselves, and not just by the experience of risk or threat, but also by subsequent actions that threaten the very system of agreed-upon meanings that allow a complex social system to function. (as quoted in Freudenburg & Jones, 1991, p. 1159)

The second conceptual tool, *atrophy of vigilance*, is the decline over time in regulatory surveillance. Atrophy of vigilance includes complacency ("it can't happen here" or groupthink[9]), concerns with costs and budgets that substitutes for an authentic conversation on risk, and an "expectation for organizational performance to get sloppier over time particularly in the case of rare or 'unexpected' problems'" (Freudenburg, 1992; Freudenburg & Gramling, 2011, p. 35).

First outlined in 1992 in a discussion of "*technological* risks that are in some way *managed* by humans and their institutions (governments, corporations, communities) *over time*" (p. 2), Bill identified four sets of interrelated factors "that are unintended and/or unseen" that may influence organizational functioning (p. 5). As a guidepost, these elements buttress recreancy: *individual-level human factors* (standard human factors, stochastic human factors, external human factors, pp. 6−9), *organizational factors* (e.g., "pervasive mindsets" that reflect organizational hubris, bureaucratic attenuation of information flows, diffraction of responsibility, amplified risk taking, the "specialized division of responsibility creates not just the possibility that a single weak link will cause the entire 'chain' to fall, but it also increases the possibility that one of more links will be forgotten altogether," p. 16), *atrophy of vigilance* (e.g., attentiveness and vigilance deteriorate, displacement and routinization occurs, safety measures are relegated to "non-status," pp. 20−21), and *imbalanced distribution of institutional resources*. In outlining these critical threads, Bill (1992) reminds us of several key issues: problems "can be created not just by individuals but by institutions, and not just by volitions, but by situations" (p. 5); the complexity of an organization can "create difficulties, oversights, omissions, and lacunae of responsibilities" (pp. 17−18); and that if an institution's risk management programs had "succeeded in averting the disaster, no one had would ever have 'known'" (p. 23).[10]

With the third conceptual tool, *bureaucratic slippage*, there is a "tendency for broad policies to be altered through successive reinterpretation, such that the ultimate implementation may bear little resemblance to legislated or other broad statements of policy intent" (Freudenburg & Gramling, 1994, p. 222). Slippage therefore involves "disjunctions" between laws and how a particular agency or department performs its duties (p. 222), which can give way to the "potential for considerable bureaucratic slippage between the statement of goals and the reality of implementation" (p. 232). Bureaucratic slippage, according to the authors, is a gradual process that "can resemble the childhood game in which a 'secret' is whispered to one person, who then whispers it to the next, and so on; the eventual secret, or the eventual implementation of the policy, can prove to have very little resemblance to the statement that started the process" (Freudenburg & Gramling, 1994, p. 222).

In the next section, I provide documentation and direct accounts from 9/11 hearings that give weight to Bill's conceptual tools. These materials indicate the September 11, 2001 attacks involved multiple failures within numerous federal agencies, not only those responsible for intelligence analysis[11] and production, but what is termed "finished intelligence" (Central Intelligence Agency, 1999). When the National Coordinator for Security, Infrastructure Protection, and Counterterrorism under the Clinton administration, Richard A. Clarke (2008) was queried by the 9/11 Commission if he thought the September 11, 2001 attacks were an intelligence failure, he replied:

> …That it had not been a failure to provide strategic warning that al Qaeda existed and was intent on attacking us. The message had loudly and repeatedly been given to the leadership of the Bush administration, who for all practical purposes ignored it. But 9/11 was clearly an intelligence failure at the tactical level, since the intelligence agencies were unable to tell us when, where, how, or who was going to attack us. In short, they provided me with no actionable intelligence, nothing to utilize to preempt the attack. (pp. 118–119)[12]

A few words on underlying intent of this discussion: My brief descent into the historical record of 9/11 is not designed to be an exhaustive risk analysis of the disaster, nor how Bill's theories intersect with each finding by committees and commissions that studied the September 11 attacks. In addition, my discussion does not address various conspiracy (alternative) theories surrounding 9/11 but instead documents the "repeated incompetence" (Clarke, 2008, p. 170) over a period of years across federal agencies and presidential administrations in failing to map terrorist events from the first Word Trade Center bombing (1993), the Khobar Towers bombing (1996), Kenyan and Tanzanian embassy bombings (1998), and attack on the USS Cole (2000) to a set of actors. Nor is this discussion focused on blaming one agency, department, or set of individuals. Drawing on Freudenburg's (1993), "it is not relevant to know whether or not villainy can be discerned, whether at individual or collective levels; instead to use Weber's words, the key question is simply whether experience shows that the behaviors of specialized individuals and institutions can be counted on" (p. 917).

CONCEPTUAL TOOLS, MEET THE IC

Through Max Weber's (1978) work on rationality or verifiable certainty,[13] and the division and specialization of labor, Bill refined his thoughts on risk and recreancy. In making the following observation, Bill pinpointed the possible roots of disaster within a particular element of Weber's bureaucracy:

> Society is not so much infallibility as something far more paradoxical. Our current division of labor permits a level of prosperity, prowess, and even physical health and safety, that is altogether unprecedented. The same division of labor, however, may increase societal vulnerability to cases where duties are not being carried out properly – whether the "fault" is one of individual actors or of a broader system in which important responsibilities may fall through the institutional cracks. (1993, p. 915)

Although Bill is referring to the failure of institutions to respond to risks and accidents posed by technology in the above quote, recreancy, atrophy of vigilance, and bureaucratic slippage each offer an avenue of analysis into information flows and decision making processes relative to risks and threats, autonomy (agency), and action (or inaction). When viewed as a package, these tools offer plasticity to investigators who wish to probe the further reaches of institutional collapse, including historical contexts, knowledge production, internal decision making, policy dynamics, and influence on public trust. While recreancy, atrophy of vigilance, and bureaucratic slippage are at the crux of Bill's research, and applied by him in analysis of institutional policies and environmental disasters, these tools take on a new dimension when applied to the IC and the various categories of failures it may encounter: intelligence, warning, and strategic (e.g., Brauch, 2011; Friedrich, 1972; Grabo, 2010; Greenberg, 2010; House Committee on Government Reform, 2002; Johnston, 2005; Jones, 2010; Macartney, 1988; Marin, 2004; Ransom, 1980; Riebling, 2002; Senate Select Committee on Intelligence, 1977, 2002;[14] Steele, 2002; Turner, 2005; Weiner, 2007; Zegart, 1999), and particularly the September 11 attacks (e.g., Clarke, 2004, 2008; Diamond, 2008; Edmonds, 2012; National Commission on Terrorist Attacks Upon the United States, 2004; Zegart, 2007a, 2007b).[15]

Remarkably, a tour of the research literature on the September 11 attacks does not reflect the use of Bill's conceptual tools in the analysis of the disaster. It is clear, however, that recreancy, atrophy of vigilance, and bureaucratic slippage underlie the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence (2002, 2004a, 2004b) findings and testimony as reported in the *Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001* and the unclassified version of the National Commission on Terrorist Attacks Upon the United States (2004) *Final Report*. These investigations "explained to the American people how and why the U.S. government failed to discover that terrorists, operating from Afghanistan, were infiltrating the United States in order to use a most unconventional resource – commercial airplanes – as weapons that would kill thousands of people" (Commission on the Prevention of WMD Proliferation and Terrorism, 2008, p. xii). Although George Tenet remarked to the Senate Select Committee on Intelligence (2002) that "when people use the word 'failure,' 'failure' means no focus, no attention, no discipline – and those were not present in what either we or the FBI did here and around the world" (p. 136), findings and accounts included in this discussion bear out the bureaucratic miasma preceding the 9/11 attacks. To quote one former CIA analyst, an intelligence failure is a "number of little failures that cluster into an *enormous failure*" (Mahle, 2004, p. 11).

However one chooses to characterize the 9/11 attacks and the sheer inability and ineffectiveness of the federal government to institute emergency measures to prevent the murder of approximately three thousand people, the release of a myriad of chemicals into the environment and subsequent environmental illnesses to first responders and the public, and on and on, it is worth noting when

> Failures occur, they are likely to involve bureaucratic politics and occur at the policy-intelligence interface, where good intelligence is most important but also most vulnerable. Policymakers and intelligence producers who would avoid future "intelligence failures" need to be aware of the bureaucratic pitfalls inherent in their relationship. (Macartney, 1988, p. 14)

Let us begin linking Bill's conceptual tools with the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence, known as the Joint Inquiry. There are two sets of hearings (September, Volume 1 and October, Volume 2) held in 2002 and published in 2004. A classified version of the hearing was declassified in 2002. The Joint Inquiry attempted to identify root causes of the 9/11 attacks. I draw from all three documents below.

The first example of recreancy, atrophy of vigilance, and bureaucratic slippage have origins in the 1993 World Trade Center bombing. At the Joint Inquiry hearing, George Tenet testified that "a common thread runs between the first attack on the World Trade Center in February 1993 and the 11 September attacks" (p. 129). While Tenet identified a link between the 1993 bombings and September 11 attacks, the Joint Inquiry "found no evidence that, before September 11, analysts in the Intelligence Community were cataloguing information regarding the use of airplanes as weapons as a terrorist tactic; sending requirements to collectors to look for additional information on this threat; or considering the likelihood that Bin Laden, al-Qa'ida, or any other terrorist group, would attack the United States or U.S. interests in this way" (Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence, 2002, p. 214).

Ms. Eleanor Hill, Staff Director for the Joint Inquiry, testified that she and her staff interviewed officials at the Department of Defense, Treasury, State, Justice, Transportation, Energy, and private sector organizations regarding the 9/11 attacks. Hill reported to the Joint Inquiry that her staff focused on the Central Intelligence Agency (CIA), Federal Bureau of Intelligence (FBI), and National Security Agency (NSA) "where the most extensive universe of potentially relevant intelligence resides" (Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence, 2004a, p. 62).[16] Hill reported her research team was (emphasis added)

> Able to determine to date, the Intelligence community did have general indications of *a possible terrorist attack against the U.S. or U.S. interests overseas in the spring and summer of 2001 and promulgated strategic warnings*. However, it does not appear to date that the Intelligence community had information prior to September 11 *that identified where, when, and how the attacks would be carried out*. (Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence, 2004a, p. 64)[17]

At the same hearing on September 18, the testimony of Ms. Kristen Breitwiser, co-chairperson of the September 11 Advocates, offers a divergent account. Based on open source, public information, Breitwiser's comments are a veritable literature review of threats and warnings compiled by a myriad of federal agencies preceding the attack (2004a, pp. 21–47) that implies a multi-tiered institutional collapse. That is, 9/11 did not occur due to the malfunction of *one* federal agency, subdepartment, hive, or individual in anticipating the finer details of the attacks; numerous federal units across presidential administrations were unable to entirely "grok" a time, place, and extent of the attacks.

In his research, Bill used Lee Clarke's (1999) concept of the fantasy document or "rationality badges, symbols organizations use to signal they are in control of danger…they are usually set in a rhetoric of technical competence" (p. 16) as a vehicle to explore failure through administrative communications. It seem fitting to carry on this tradition with Presidential Decision Directive 62 or PDD-62. This PDD plays a key role in the U.S. government's inability to insert policy into interagency action to circumvent 9/11 and remains classified (White House, 1998) with sections redacted and released through the Joint Inquiry *Report* published in December 2002 with additional commentary and documents. The Joint Inquiry identified key challenges of PDD-62, a “fantasy document”: that was not widely acknowledged in federal circles as a basis for operations and policy:

> The DCI’s December 1998 declaration was remarkable for its foresight and aggressiveness. *But it could only have effect within a limited sphere because coordinating the U.S. Government’s response to the Bin Ladin threat was not the responsibility of the DCI or the Intelligence Community, but of the President and the National Security Council.*
>
> In a Joint Inquiry briefing, Mr. (Richard A.) Clarke touched on this issue when he discussed Presidential Decision Directive 62, “Protection Against Unconventional Threat to the Homeland and Americans Overseas.” That PDD was signed by President Clinton in May 1998, before the bombings of the two U.S. Embassies in Africa and before the DCI’s declaration of war. According to Mr. Clarke, the PDD created a ten-program counterterrorism initiative and assigned counterterrorist responsibilities to specific agencies.
>
> Within that effort were the seeds of an integrated, comprehensive government-wide strategy for countering the Bin Ladin threat that could have put the nation on a war footing before September 11. *The initiative is perhaps the closest that President Clinton and the National Security Council came between 1998 and the Administration’s departure from office in January 2001 to a coordinated response to the threat.* However, the PDD does not appear to have had much impact. It is clearly not as straightforward as the DCI’s declaration and, *beyond Mr. Clarke’s* [sic, Richard A.] *reference to it in his testimony, no other Joint Inquiry witness pointed to PDD-62 as the policy guiding the government’s response to the growing al-Qa’ida threat.* (Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence, 2002, pp. 234–235)

PDD-62 remains classified (White House, 1998) with sections redacted and released through the Joint Inquiry *Report*. Its existence is significant for two reasons: first, the discussion of the DCI’s 1998 declaration, when contrasted with testimony from Ms. Hill at the open, public September hearings is stunning. Hill reported that while the NSA was cognizant of Tenet’s December 1998 “declaration of war,” “relatively few of the FBI agents interviewed by the Joint Inquiry seem to have been aware” of the memo (Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence, 2004a, pp. 101–102). Ignorance of the Tenet declaration across the federal bureaucracy caused a domino effect that influenced the intelligence abilities of Joint Terrorism Task Forces (JTTFs) around the country and to “mobilize a public awareness and to harden the homeland” (Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence, 2004a, p. 102); and second, PDD-62 is central to understanding distinct terrorism-related duties assigned to specific federal agencies by the National Security Council. For example, the Department of Justice was tasked with "apprehension, extradition, rendition, and prosecution" and "countering the foreign terrorist threat in the United States"; the Department of State with "international cooperation"; the CIA with "disruption"; Department of Transportation, transportation security; and the National Security Council in "preventing terrorist acquisition of weapons of mass destruction" and "protection of critical infrastructure and cybersystems" (Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence, 2002, pp. 234–235).

To further support the notion of a system-wide collapse, we look again to Eleanor Hill and her research team, who reported that

> While the FAA, the Customs Service, the State Department and INS each had data concerning the 19 hijackers, that data was not related to their terrorist activities or associations. As a result, none of this information would, by itself, have aroused suspicions regarding a planned terrorist attack within the United States. Instead, these agencies had routine information concerning the vital statistics, travel, immigration and medical status of some of the hijackers. (Senate Select Committee on Intelligence and Permanent Select Committee on Intelligence, 2004b, p. 100)

Moreover, following the September 11 attacks a "focused CIA review of over 1,500 Classified Intelligence Reports that had not previously been provided to the State Department for watchlist purposes resulted in the identification of 150 suspected terrorists and the addition of 58 suspected terrorist names to the watchlist" (Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence, 2002, p. 35–36).

One of the most dramatic cases of failed interagency (risk) communication reported at the Joint Inquiry hearings was the "Phoenix memo," or the "Phoenix Electronic Communication" of July 10, 2001, discussed by both Ms. Hill and Ms. Breitwiser. The memo was filed by FBI Agent Kenneth Williams,[18] of the Phoenix division, to the Usama Bin Laden and Radical Fundamentalist Unit within the FBI headquarters' Counterrorism Division and the FBI's New York Field Office. The memo stated concern that an "inordinate number of individuals of investigative interest" were attending civil aviation training in Arizona. The EC also contained recommendations for action (Select Committee on Intelligence and Permanent Select Committee on Intelligence, 2004a, p. 437). Ms. Hill concluded that throughout the Joint Inquiry review, her team of investigators "found that the FBI's ability to handle strategic analytic products, such as the Phoenix EC, was at best, limited…inadequate information sharing within the FBI, particularly between operational and analytic units" (Select Committee on

Intelligence and House Permanent Select Committee on Intelligence, 2004a, p. 437). Further, Hill's and the Joint Inquiry research team discovered that

> Given the lack of information sharing across units in FBI headquarters, personnel who saw the Phoenix memo had no knowledge of any prior instances [*sic*, FBI investigations] involving terrorist groups. Since the prior reporting did not directly relate to al-Qa'ida, they were unable to evaluate the Phoenix EC in the context of what was known… (Select Committee on Intelligence and House Permanent Select Committee on Intelligence, 2004a, p. 438)

The Federal Aviation Administration (FAA) was not given a copy of the Phoenix memo prior to the attacks, "and still did not have a copy two weeks after the matter had become public in early 2002" (Select Committee on Intelligence and House Permanent Select Committee on Intelligence, 2004b, p. 101).

Perhaps the FBI's recreancy, atrophy, and slippage were in part due to information overload and excessive bureaucratization (Friedrich, 1972, p. 218), "bureaucratic faultlines" "where major agencies have overlapping responsibilities and fundamental differences in outlook" (Lord, 1988, p. 37),[19] IC-wide budget cuts imposed by policymakers that influenced information sharing (Select Committee on Intelligence and House Permanent Select Committee on Intelligence, 2004a, pp. 161, 218, 615–616) and additional lack of resources, including agents, analysts, linguists, and technology,[20] might have also contributed to the inability of the Bureau to respond preemptively to prevent the attacks. Or yet, perhaps it is a case described by former FBI Director Louis J. Freeh of complying with "the rules as they were given to us by the Attorney General and the Congress." For example, FBI agents were not permitted, "without special circumstances, to visit a suspect group's Web site or to attend its public meetings. Counterintelligence, domestic terrorism and informant guidelines promulgated years ago and updated with new restrictions curtailed our ability to collect information in national security cases" (Select Committee on Intelligence and House Permanent Select Committee on Intelligence, 2004b, p. 492). As an unnamed FBI Headquarters agent reported to the Joint Inquiry – and this harkens to the etymology of recreancy as *defeat and surrender* – he

> Witnessed first hand a dedicated group of counterterrorism professionals that have been routinely overwhelmed by large caseloads and continual crisis management. They also confront the daily frustrations posed by limited resources, especially within our analytical ranks, and inadequate technology, which hampers their ability to communicate within FBI headquarters, with our 56 field divisions and 44 legal attaches around the world, as well as with other elements of the law enforcement and intelligence

> community. (Select Committee on Intelligence and Permanent Select Committee on Intelligence, 2004a, p. 485)

Recalling our earlier discussion of Bill's "principles" that influence organizational functioning, this unidentified FBI agent's account suggests that recreancy can happen on differing levels. Recreancy can reflect an *internal* failure of institutions to the safeguard its working parts and provide sustenance to its divisions. That is, lack of institutional support within the FBI that addressed the *imbalanced distribution of institutional resources* (Freudenburg, 1992), led to an overpowering effect, an overwhelming, with subsequent inability of agents to fully respond to the daily, exhaustive management of crises.

Another unnamed FBI agent who testified at the Joint Inquiry reported that pre-9/11 "no criminal investigator was able to read any SIGINT information. And that was, in my personal opinion, way too high of a wall with regards to that, because that was something that we relied on from a perspective just to kind of point us in the right direction" (Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence, 2004a, p. 422). This may seem an insignificant finding, but SIGNIT or *signals intelligence*, as a category of intelligence is "either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted" (Department of Defense, 2010) is *intelligence information*, and as such, utilized by both the FBI and other members of the IC in the intelligence cycle (planning, collection, processing, production, and dissemination) or the process where information is acquired and converted to intelligence.[21]

The National Commission on Terrorist Attacks Upon the United States, or Kean Commission, validated many of the same details as reported in the Joint Inquiry, such as "the most serious weaknesses in agency capabilities were in the domestic arena…the FBI, the Immigration and Naturalization Service, the FAA, and others" (p. 352). The Kean Commission also observed the 9/11 attacks revealed four kinds of failures: in imagination, policy, capabilities, and management" (p. 339). Further, the Commission, in a most sociological, Weberian observation, stated that "imagination is not a gift usually associated with bureaucracies" (National Commission on Terrorist Attacks Upon the United States, 2004, p. 344).

The Commission's *Final Report*, especially its endnotes, is a litany of failures of imagination by various agencies to meet the challenges of global terrorism across presidential administrations. However, it is critical to list further examples from the Commission's report in order to support the interlocking nature of Bill's (and Gramling's) ideas on recreancy, atrophy of vigilance, and bureaucratic slippage. First a July, 1995 National Intelligence Estimate (NIE) predicted terrorist-related attacks against and in the Unites States and "specified particular points of vulnerability" such as the "White House, Capitol, symbols of capitalism such as Wall Street…" (p. 341); secondly, the Commission substantiated the Joint Inquiry findings that threat reports were issued as early as 1998 (p. 344). Additional examples from the 9/11 Commission's *Final Report* include (emphasis added):

- FBI officials did not receive the *President's Daily Brief* (*PDB*) – the daily intelligence briefing consisting of six issues considered significant by CIA staff (p. 209); the Attorney General, FBI Director, and Richard Clarke, the National Security Council counterterrorism coordinator all received the *Senior Executive Intelligence Briefing* (SEIB) but not the *PDB* (p. 255). Further, while Clarke and his staff "had extensive access to terrorism reporting, but they did not have access to internal nondisseminated information" from the NSA, CIA, or FBI (p. 255).
- The CIA did not write any analytical assessments of possible hijacking scenarios (vulnerabilities, p. 345).
- The Director of Central Intelligence (DCI) Robert Gates proposed *several recommendations in 1992* including "strengthening the national intelligence officer for warning" (p. 346). The Kean Commission "*was told these measures languished under Gate's successors and responsibility for warning related to a terrorist attack passed from the national intelligence officer for warning to the CTC* (CIA Counterterrorism Center). An Intelligence Community Counterterrorism Board had the responsibility to issue threat advisories. With the important exception of analysis of al Qaeda efforts in chemical, biological, radiological, and nuclear weapons, we did not find evidence that the methods to avoid surprise attack that had been so laboriously developed over the years were regularly applied" (vulnerabilities, p. 347).
- *Neither the intelligence community nor aviation security experts analyzed systemic defenses within an aircraft or against terrorist controlled aircraft suicidal or otherwise*. The many threat reports were passed to the FAA. While that agency continued to react to specific, credible threats, it did not try to perform the broader warning functions we describe here. No one in government was taking on the role for domestic vulnerabilities (p. 347).

BUILDING ON BILL'S RESEARCH

In concluding my brief discussion of Freudenburg's conceptual tools and their use in understanding the 9/11 disaster, there are two thoughts worth voicing. First, Bill's numerous works on risk, especially in the areas of risk analysis, risk communication, risk perception, and probabilistic risk assessment (as reported on his Curriculum Vitae, this volume) can not only offer the IC a thoughtful, additional means to reflect on risk but its problematics.

Second, and here I close my discussion on recreancy, atrophy of vigilance, and bureaucratic slippage with Bill's words (2001) on what I believe should be added to his conceptual toolbox: *hypervigilance*. I am aware, Bill doesn't mention the concept in his work, but hypervigilance as suggested in the context of post-9/11 carries with it the extreme ends taken by federal and congressional bodies to stem attacks domestically and around the globe.

The post-September 11 landscape witnessed not only a massive reorganization of the Executive Branch with the creation of the Department of Homeland Security, but deepened intelligence gathering and surveillance through the USA PATRIOT Act, P.L. 107-56, reorganized the IC through the Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458, and granted telecommunications carriers immunity for cooperation with authorities through the FISA Amendments Act of 2008. In addition, the National Defense Authorization Act for Fiscal Year 2012 (NDAA) Subtitle D. "Counterterrorism," § 1021 establishes an "Affirmation of Authority of the Armed Forces of the United States to Detain Covered Persons Pursuant to the Authorization for Use of Military Force." Under NDAA § 1021(b)(2) a "covered person" is described as an individual who participated in the 9/11 attacks in some way, as well as a "person who was a part of or substantially supported al-Qaeda, the Taliban, or associated forces that are engaged in hostilities against the United States or its coalition partners, including any person who has committed a belligerent act or has directly supported such hostilities in aid of such enemy forces." A lawsuit filed by a group of journalists, professors, and rights activists, *Christopher Hedges, et al. v. Barack Obama, et al.* (2012), argues that under § 1021(b)(2), a covered person is "an undefined, amorphous and potentially broad class of persons engaged in protected advocacy activity." As this chapter is published, the results of the lawsuit remain undetermined, but the implications of the "covered person" category raises deep concerns as to the right to political speech and freedom of expression.

In the wake of these laws and scores of other regulatory and legal advances, increased assaults on civil liberties and human rights have occurred in the United States and abroad. Domestic and international laws have been widely interpreted by various federal, state, and local bodies as to create a type of recreancy not of a failure to *meet* responsibilities, but recreancy resulting from *overzealous attempts* to protect the public from risk of catastrophic events. Perhaps I read into Bill's words, but I can't help but think he might comment on the current atmosphere so centered on "getting it right this time" that it tramples the very footing on which public trust is based. In lieu of any direct observations from Bill on the matter, I offer final words from our colleague that reflect the essential ingredients of not only managing risk and building public trust, but democracy-building:

> Instead, most citizens' calls for "scientific" decisions are actually a request for something else – most often, for ways of assuring that "the human element" of societal decision-making will be not just technically competent, but equitable, fair, and responsive to deeply felt concerns. ln most cases, what is important is not just technical expertise, but the broader ability to expect that the "responsible" authorities will in fact behave responsibly – making decisions that will not work to the detriment of the broader society for the benefit of the few, for example, and taking care not to ignore the values that affected citizens hold to be most dear. (Freudenburg, 2001, p. 103)

NOTES

1. Kathleen Tierney (2012) does suggest that Bill's recreancy holds promise in framing "natural disasters, Y2K, terrorism, exotic disease agents, genetically modified organisms and other emerging technologies, sexually predatory Catholic priests, and the operation of global financial markets and institutions" (p. 61).

2. For a complete list of federal agencies that comprise the IC pre-9/11, see Davis (2002); post September 11, see the Director of National Intelligence, http://www.dni.gov/index.php/intelligence-community/members-of-the-ic

3. See Morgeson and colleagues (2011)'s *Doctrinal guidelines for quantitative vulnerability assessments of infrastructure-related risks* for a review of "doctrinal guidelines for quantitative vulnerability" including discussion of scenarios and risk methodologies. Also see Department of Homeland Security (2010) *Risk lexicon*, which is a controlled vocabulary derived from "directives, glossaries, and other procedural or guidance documents. In addition, RMA staff review foundational homeland security policy and doctrine to identify and collect relevant definitions" (p. 3).

4. *Risk assessment* is defined as: 1. A deliberate, analytical approach to identify which threats can exploit which vulnerabilities in an organization's specific assets. Variables should be ranked according to predetermined criteria, such as the probability of a threat targeting a specific asset or the impact of a vulnerability being

exploited by a specific threat. The assessment results in a prioritized list of risks that can be used to select safeguards to reduce vulnerabilities by creating levels of protection. 2. The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. 3. The process of evaluating security risks based on analyses of threats, vulnerabilities, and probable adverse consequences to a facility, system, or operation (Goldman, 2011).

5. The term *Intelligence failure* is controversial; Mahle (2004) describes it as "to be considered an intelligence failure, the issue must be significant in terms of national security and have an impact on U.S. interests, facilities, and citizens" (p. 11); intel failures are "often used to lay blame on the intelligence community when an unexpected event or action occurs that may have an impact of foreign policy; any misunderstanding of a situation that leads a government or its military forces to take actions that are inappropriate and counterproductive to its own interests…not all intelligence failures are warning failures" (Goldman, 2006; Joint Military Intelligence College, 2001). *Warning failure* is "often related to the failure to forecast events before they happen" (Goldman, 2006; Joint Military Intelligence College, 2001). Richard A. Clarke (2008) uses the term national security intelligence failure but does not define. Perhaps its roots go to "national security intelligence," defined as the "collection and analysis of information concerned with the relationship and homeostasis of the United States with foreign powers, organizations, and persons with regard to political and economic factors as well as the maintenance of the United States' sovereign principles. It embodies both policy intelligence and military intelligence" (Goldman, 2011).

6. Ideal type as outlined by Max Weber as a "conceptual tool to approach reality and in this sense it is 'conceptual construct'…the introduction of the ideal type is often the first step in analysis" (Swedberg, 2005, p. 120).

7. Bill's conceptual tools share in common six failures or "pathologies" that can befall organizations. As outlined by Karl W. Deutsch (1968), they are loss of power, loss of intake (loss in the effectiveness of previously existing channels of information from the outside world, or loss of entire channels), loss of steering capacity (or the ability to modify behavior with sufficient speed and precisions), loss of depth of memory, loss of capacity for partial inner rearrangement (rigidity in learning new behavior), and loss of capacity for comprehensive, fundamental rearrangement of inner structure (pp. 221–223).

8. The use of recreancy can be found in Henry David Thoreau's *Walden* in 1854, and in a sense that both Weber and Freudenburg might have approve, in Dorman Bridgman Eaton's (1875) *The Experiment of Civil Service Reform in the United States*. Eaton was critical of "favoritism and party influence" (p. 36) and the failure of civil service reform policies "they cannot, indeed be refuted by any evidence short of that which shall present the facts, the motives, the influences, the policy, *the recreancy*, the neglects, which led to the abandonment of the experiment" (p. 2).

9. Defined as "a concept that faulty decision making occurs when a group does not consider alternatives and desires unanimity at the expense of quality decisions. Groupthink can lead to seeking out few alternative solutions because there is an illusion of invulnerability" (Goldman, 2011).

10. For example, recent revelations by NSA Director General Keith B. Alexander during the Senate Appropriations Committee hearings into NSA surveillance. On June 12, 2013, Alexander stated surveillance had prevented “dozens of attacks” (McCarthy, 2013a) and on June 18, he claimed “fifty plots worldwide” were thwarted (McCarthy, 2013b). The question remains if Alexander’s “proactive disclosures” would have been disclosed by federal officials if not for the Snowden leak.

11. Intelligence analysis is the application of individual and collective cognitive methods to weigh data and test hypotheses within a secret socio-cultural context (Johnston, 2005, p. 4).

12. A transcript of Clarke’s (March 24, 2004) testimony is available at CNN, http://transcripts.cnn.com/TRANSCRIPTS/0403/24/bn.00.html

13. For an excellent review of Weber’s use of rationality across his many works, see Swedberg (2005).

14. Especially see the testimony of Eleanor Hill, Staff Director, Joint Inquiry, who outlines in detail previous failures within the IC and the Intelligence Committee’s knowledge of a possible threat of an attack in the United States (p. 73).

15. Amy Zegart (2007b) employs *adaptation failure* or the “rate of change within an organization to keep pace (or lags behind) the rate of change in the external environment” (p. 20) to characterize the IC’s response to 9/11. Zegart states that “many intelligence officers and policymakers recognized the threat, but were unable to get the intelligence reforms they believed were vital several years before 9/11” (p. 21).

16. For history and background of the Joint Inquiry and its researchers, see Best (2003).

17. Former Defense Intelligence Agency analyst Cynthia Grabo (2010) defines warning intelligence as a specialized type of knowledge; warning intelligence or “indications intelligence is concerned with those pieces of information which relate to what the enemy is or possibly is preparing to do….an ‘indication’ is a sign, a symptom, a suggestion, a ground for inferring, a basis for believing, or the like” (pp. 9−10).

18. Agent Williams was interviewed by the Joint Inquiry in a closed session.

19. Lord also discusses the “political-military faultlines” that exist between the president, National Security Council, Department of Defense, and the IC.

20. See the testimony of FBI Director Louis J. Freeh, Select Committee on Intelligence and House Permanent Select Committee on Intelligence (2004b, pp. 485, 490).

21. The FBI has a six-step intelligence cycle (see http://www.fbi.gov/about-us/intelligence/intelligence-cycle) and other members of the IC, including the CIA and DoD, a five-step cycle (Goldman, 2011). For a critique of the cycle, see Hulnick (2013) and Nolte (2010).

ACKNOWLEDGMENTS

The author thanks Bob Gramling Ph.D., Emeritus Professor of Sociology, University of Louisiana at Lafayette, Jan Goldman, Ed.D., Georgetown

University, Ivan Greenberg Ph.D., and Peter Phillips Ph.D., Sonoma State University, for their comments and suggestions on this chapter.

REFERENCES

Barber, B. (1983). *The logic and limits of trust*. New Brunswick, NJ: Rutgers University Press.

Best, R. A. (2003). The intelligence community and 9/11: Congressional hearings and the status of the investigation. *CRS Report to Congress*, January 16. RL31650. Retrieved from www.fas.org/irp/crs/RL31650.pdf. Accessed on June 19, 2013.

Brauch, H. G. (2011). Security threats, challenges, vulnerabilities and risks in U.S. national security documents. *Hexagon Series on Human and Environmental Security and Peace*, *5*, 249−274.

Central Intelligence Agency. (1999). *A consumer's guide to intelligence: Gaining knowledge and foreknowledge of the world around us*. Washington, DC: Government Printing Office, Office of Public Affairs.

Christopher Hedges et al. v. Barack Obama et al. (2012, July 2). *Plaintiffs' memorandum in support of motion for permanent injunction*. Retrieved from https://www.stopndaa.org/documents/memo-in-support-ofpermanent-injunction

Clarke, L. (1999). *Mission improbable: Using fantasy documents to tame disaster*. Chicago, IL: University of Chicago Press.

Clarke, R. A. (2004). *Against all enemies: Inside America's war on terror*. New York, NY: Free Press.

Clarke, R. A. (2008). *Your government failed you: Breaking the cycle of national security disasters*. New York, NY: Ecco.

Commission on the Prevention of WMD Proliferation and Terrorism. (2008). *World at risk*. New York, NY: Vintage Books.

Davis, L. E. (2002). *Organizing for homeland security*. RAND. Retrieved from www.rand.org/pubs/issue_papers/IP220/index2.html. Accessed on June 19, 2013.

Department of Defense. (2010). *Department of defense dictionary of military and associated terms*. JP 1-02. Amended through June 15, 2010. Retrieved from www.dtic.mil/doctrine/dod_dictionary/. Accessed on July 19, 2013.

Department of Homeland Security. (2010). *DHS risk lexicon*. Risk Steering Committee. Washington, DC: U.S. Government Printing Office. Retrieved from www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf. Accessed on June 19, 2013.

Deutsch, K. W. (1968). *The nerves of government: Models of political communication and control*. New York, NY: Free Press.

Diamond, J. (2008). *The CIA and the culture of failure: U.S. intelligence from the end of the Cold War to the invasion of Iraq*. Stanford, CA: Stanford Security Series.

Eaton, D. B. (1875). *The experiment of civil service reform in the United States: Its methods, its effects, and the excuses and responsibility for its abandonment, set forth in a paper*. Detroit. Retrieved from googlebooks: https://tinyurl.com/m2ot3m2. Accessed on June 16, 2013.

Edmonds, S. (2012). *Classified woman: The Sibel Edmonds story: A memoir*. Alexandria, VA: Sibel Edmonds.

Freudenburg, W. R. (1992). Nothing recedes like success? Risk analysis and the organizational amplification of risks. *Risk: Issues in Health and Safety*, *3*(1), 1−35.

Freudenburg, W. R. (1993). Risk and recreancy: Weber, the division of labor, and the rationality of risk perceptions, *Social Forces*, 71(4), 909−932).

Freudenburg, W. R. (1996a). Risky thinking: Irrational fears about risk and society. *Annals of the American Academy of Political and Social Science*, *545*, 44−53.

Freudenburg, W. R. (1996b). Strange chemistry: Environmental risk conflicts in a world of science, values, and blind spots. In C. Richard Cothern (Ed.), *Handbook for environmental risk decision making: Values, perceptions and ethics* (pp. 11−36). Boca Raton, FL: Lewis Publishers.

Freudenburg, W. R. (2001). Risk, responsibility and recreancy. *Research in Social Problems and Public Policy*, *9*, 87−108.

Freudenburg, W. R., & Gramling, R. (1994). Bureaucratic slippage and failures of agency vigilance: The case of the environmental studies program. *Social Problems*, *41*(2), 214−239.

Freudenburg, W. R., & Gramling, R. (2011). *Blowout in the gulf: The BP oil spill disaster and the future of energy in America*. Cambridge, MA: MIT Press.

Freudenburg, W. R., & Jones, T. R. (1991). Attitudes and stress in the presence of technological risk: A test of the Supreme Court hypothesis. *Social Forces*, *69*(4), 1143−1168.

Friedrich, C. (1972). *The pathology of politics*. New York, NY: Harper Row.

Goldman, J. (2006). *Words of intelligence: A dictionary*. Lanham, MD: Scarecrow Press.

Goldman, J. (2011). *Words of intelligence: An intelligence professional's lexicon for domestic and foreign threats*. Lanham, MD: Scarecrow Press.

Grabo, C. (2010). *Handbook of warning intelligence: Assessing the threat to national security*. Lanham, MD: Scarecrow Press.

Greenberg, I. (2010). *The dangers of dissent: The FBI and civil liberties since 1965*. Lanham, MD: Lexington Books.

Homeland Security Presidential Directive 7. (2003, December 17). *Critical infrastructure identification, prioritization, and protection*. Retrieved from www.dhs.gov/homeland-security-presidential-directive-7. Accessed on July 14, 2013.

House Committee on Government Reform. (2002). *Is the CIA's refusal to cooperate with congressional inquiries a threat to effective oversight of the operations of the federal government*? Joint hearing before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations and the Subcommittee on National Security, Veterans Affairs, and International Relations of the Committee on Government Reform, House of Representatives, 107th Congress, first session, July 18, 2001. Washington, DC: U.S. Government Printing Office.

Hulnick, A. (2013). Intelligence theory: Seeking better models. In M. Phythian (Ed.), *Understanding the intelligence cycle* (pp. 149−158). Milton Park, Abingdon, UK: Routledge.

Johnston, R. (2005). *Analytic culture in the US intelligence community: An ethnographic study*. Center for the Study of Intelligence, Central Intelligence Agency. Washington, DC: U.S. Government Printing Office. Retrieved from http://permanent.access.gpo.gov/lps64831/CIA%201929667132.pdf. Accessed on June 17, 2013.

Joint Military Intelligence College. (2001, October). *Intelligence warning terminology*. Washington, DC: Defense Intelligence Agency.

Jones, I. (2010). *The human factor: Inside the CIA's dysfunctional intelligence culture*. New York, NY: Encounter Books.

Lord, C. (1988). *The presidency and the management of national security*. New York, NY: Free Press.

Macartney, J. (1988). Intelligence and bureaucratic politics. Declassified, based on a paper presented at the annual meeting of the American Political Science Association in Washington, DC. Retrieved from media.nara.gov/dc metro/rg-263/6922330/Box-10-121-2/263-a1-27-box-10-121-2.pdf. Accessed on June 19, 2013.

Mahle, M. B. (2004). *Denial and deception: An insider's view of the CIA*. New York, NY: Nation Books.

Marin, S. (2004). Preventing intelligence failures by looking at the past. *International Journal of Intelligence and Counterintelligence*, *17*, 655–672.

McCarthy, T. (2013a, June 12). NSA director: Surveillance helped stop 'dozens of terrorist events' – As it happened. *The Guardian*. Retrieved from www.theguardian.com/world/2013/jun/12/edward-snowden-hongkong-live#block-51b8e05ae4b0bf6d0fdbdbc0. Accessed on August 8, 2013.

McCarthy, T. (2013b, June 18). NSA chief says exposure of surveillance programs has 'irreversible' impact – As it happened. *The Guardian*. Retrieved from www.theguardian.com/world/2013/jun/18/nsa-chief-house-hearingsurveillance-live. Accessed on August 8, 2013.

Morgeson, J. D., Brooks, P. S., Disraelly, D. S., Erb, J. L., Neiman, M. L., & Picard, W. C. (2011). Doctrinal guidelines for quantitative vulnerability assessments of infrastructure-related risks. Volume I. Institute for Defense Analyses IDA Document D-4477. Retrieved from www.dtic.mil/cgi bin/GetTRDoc?AD = ADA558820. Accessed on June 15, 2013.

National Commission on Terrorist Attacks Upon the United States. (2004). *9/11 report (Final report)*. Washington DC: Government Printing Office. Retrieved from www.9-11commission.gov/report/911Report.pdf. Accessed on July 12, 2013.

National Defense Authorization Act for Fiscal Year. (2012). *H. R. 1540. 112th Congress, First session*. Retrieved from http://www.gpo.gov/fdsys/pkg/BILLS112hr1540enr/pdf/BILLS-112hr1540enr.pdf

Nolte, W. M. (2010). Intelligence analysis in an uncertain environment. In L. K. Johnson (Ed.), *The Oxford handbook of national security intelligence* (pp. 404–421). New York, NY: Oxford University Press.

Office of Management and Budget. (1996). *Management of federal information resources*. Circular No. A-130. February 8. Retrieved from www.whitehouse.gov/omb/circulars_a130. Accessed on July 19, 2013.

Oxford English Dictionary. (2013). *Recreancy*. New York, NY: Oxford University Press.

Ransom, H. H. (1980). Being intelligent about secret intelligence agencies. *The American Political Science Review*, *74*(1), 141–148.

Riebling, M. (2002). *Wedge: From Pearl Harbor to 9/11, how the secret war between the FBI and CIA has endangered national security*. New York, NY: Simon and Schuster.

Senate Select Committee on Intelligence. (1977). *Project MKULTRA, the CIA's program of research in behavioral modification: Joint hearing before the Select Committee on Intelligence and the Subcommittee on Health and Scientific Research of the Committee on Human Resources*, United States Senate, 95th Congress, 1st session, August 3. Washington, DC: Government Printing Office.

Senate Select Committee on Intelligence. (2002). *Current and projected national security threats to the United States*. S. HRG. 107–597, 107th Congress, 2nd session, February 6. Washington, DC: Government Printing Office. Retrieved from www.intelligence.senate.gov/107597.pdf. Accessed on August 5, 2013.

Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence. (2002). *Joint inquiry into intelligence community activities before and after the* *terrorist attacks of September 11, 2001. Report of the U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence together with additional views*. Senate Rpt. 107-351, 107th Congress, 2nd session, H. Rpt. 107-792. December. Washington, DC: Government Printing Office.

Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence. (2004a). *Joint inquiry into intelligence community activities before and after the terrorist attacks of September 11, 2001: Hearings before the Select Committee on Intelligence*. S. HRG. 107-1086, Vol. 1. September 18, 19, 20, 24, 26, 2002. Washington, DC: Government Printing Office. Retrieved from www.gpo.gov/fdsys/pkg/CHRG107jhrg96166/pdf/CHRG107jhrg96166.pdf. Accessed on June 15, 2013.

Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence. (2004b). *Joint inquiry into intelligence community activities before and after the terrorist attacks of September 11, 2001: Hearings before the Select Committee on Intelligence*, October 1, 3, 8, 17, 2002. S. HRG. 107-1086, Vol. 2. Washington, DC: Government Printing Office. Retrieved from www.intelligence.senate.gov/pdfs/1071086v2.pdf. Accessed on June 15, 2013.

Steele, R. D. (2002). Crafting intelligence in the aftermath of disaster. *International Journal of Intelligence and Counterintelligence*, *15*, 161–178.

Swedberg, R. (2005). *The Max Weber dictionary*. Stanford: Stanford University Press.

Tierney, K. (2012). A bridge to somewhere: William Freudenburg, environmental sociology, and disaster research. *Journal of Environmental Studies and Sciences*, *2*, 58–68.

Turner, M. A. (2005). *Why secret intelligence fails*. Dulles, VA: Potomac Books.

Warner, M. (2009). Intelligence as risk shifting. In P. Gill, S. Marrin, & M. Phythian (Eds.), *Intelligence theory: Key questions and debates* (pp. 16–32). New York, NY: Routledge.

Weber, M. (1958). *From Max Weber: Essays in sociology* (H. H. Gerth & C. Wright Mills, Eds. and Trans.). New York, NY: Oxford University Press.

Weber, M. (1978). *Economy and society: An outline of interpretive sociology* (E. Fischoff, Trans.; G. Roth & C. Wittich, Eds.). Berkeley, CA: University of California Press.

Weiner, T. (2007). *Legacy of ashes: The history of the CIA*. New York, NY: Doubleday.

White House. (1998). *Fact sheet: Combatting terrorism, Presidential Decision Directive 62*. Retrieved from www.fas.org/irp/offdocs/pdd-62.htm. Accessed on August 5, 2013.

Zegart, A. (1999). *Flawed by design: The evolution of the CIA, JCS, and NSC*. Stanford, CA: Stanford University Press.

Zegart, A. (2007a). 9/11 and the FBI: The organizational roots of failure. *Intelligence and National Security*, *22*(2), 165–184.

Zegart, A. (2007b). *Spying blind: The CIA, FBI, and the origins of 9/11*. Princeton, NJ: Princeton University Press.