Government Information Quarterly 32 (2015) 342–352

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

U.S. homeland security and risk assessment

Philip Doty

School of Information, University of Texas at Austin, 1616 Guadalupe Street, Suite 5.202, USA

ARTICLE INFO

Article history:
Received 14 July 2014
Received in revised form 5 April 2015
Accepted 30 April 2015
Available online 15 June 2015

Keywords:
Surveillance
Risk
Homeland security
Secrecy
Governmentality
Risk society
Risk *imaginary*

ABSTRACT

Risk is constitutive of homeland security policy in the United States, and the risk apparatus supports growing concentration of executive power, increased surveillance, and secrecy. For example, the Transportation Security Administration in the Department of Homeland Security employs risk assessment particularly against groups considered "other." Using the work of mostly European scholars, especially the literatures about Foucault's governmentality and Beck's risk society, the paper combines theory with empirical work by governmental agencies on transparency, secrecy, and risk assessment methods used in the Department of Homeland Security, providing insight into the securitization of the American state. Risk is a means to *futurize* threats to the polity, to create the security *imaginary*, a *fictionalization* that creates a moral panic and a climate of fear in seeking to cope with uncertainty. With those limitations of risk in mind, we can question four important elements of risk in U.S. security practice: "connecting the dots"; the quantitative bases of risk assessment algorithms; how risk assessment tends to ignore the important if circular intentionality of terror; and the difficulties inherent in controlling populations by classification, especially other-ed populations. The paper concludes with suggestions about unmasking the uncertainty of risk assessment and enabling oversight of its practice by legislative, judicial, and public actors.

> "The secret is: *it is not the terrorist act that destroys the West, but the reaction to its anticipation*. It ignites the felt war in the minds and centres of the West."
>
> [[emphasis in the original] — Beck (2009, p. 157)]

1. Introduction

At the annual meeting of the Association for Information Science and Technology in Montréal in fall 2013, there was a panel discussion about information policy since 9/11/2001 that considered, among other things, the role of scholars in the study of public information policy and security. Among the themes discussed was the scholarly and ethical imperative for scholars of public policy to be members of "the loyal opposition," exploring what Mannheim called "dangerous thoughts" (cited in Mythen & Walklate, 2006, p. 395). That is, policy scholars must view what policy makers do with a skeptical but sympathetic eye and must be independent from governmental power while recognizing the difficult task at hand in keeping the polity safe, open, and welcoming. The current paper is an exercise in that skepticism, critically examining the use of risk management in general, and risk analysis in particular, as a cornerstone of security policy in the United States.

Post-9/11 initiatives in the U.S. to increase government secrecy and government surveillance are part of a much older and larger narrative in politics of the accretion of executive power and the intractable tension between secrecy and openness. This last is a "mess" (Schön, 1983, p. 16, citing Russell Ackoff); a "muddle" (Lindblom, 1959, 1979); or a "wicked problem" (Rittel & Webber, 1973). These are terms used to describe enduring dilemmas in public policy. One way of reading American political history is as a story of the increasing concentration of power in the executive branch of government, no matter which political party or parties are in power or which may be in decline. This concentration comes, in part, at the expense of the power of the legislature and judiciary. In the context of security affairs, one theme in this expansion is the growth of the concept of homeland security from war and national security, a story well if briefly told by Relyea (2002) in the earlier pages of this journal. Another theme is the "rhetoric of crisis" that governments of all stripes have commonly used, including the executive branch of the government of the United States, which has been explored in depth by, for example, Kiewe (1994) and Kuypers (1997) on the U.S. presidency and crisis rhetoric. This long-standing use of crisis has, since 9/11, devolved into the rhetoric of permanent emergency (Doty, forthcoming). A third theme in this expansion is how it is that increased governmental secrecy and surveillance can undermine the public trust in government.

In order to make appropriate theoretical interventions and to inform both the polity and policy makers about political conflicts, scholars must often assume a contrarian position in the emotionally volatile context of the politics of security. It is important to ask genuine questions about important security matters, especially to question the need for increased surveillance, increased secrecy about governmental actions

E-mail address: pdoty@ischool.utexas.edu.

http://dx.doi.org/10.1016/j.giq.2015.04.008
0740-624X/

and decision-making, exceptions to the Constitutional protections of citizens and non-citizens, and the purported necessity to avoid judicial and legislative review and oversight of executive action. At the same time, however, research into information policy problems can remind us all of the moral landscape in which such problems reside without resorting to moralistic and antagonistic attitudes toward decision makers.

2. Examples of risk assessment and travel security since 9/11

Acting on President George Bush's *Proposal to Create the Department of Homeland Security* of June 2002 (U.S. Executive Office of the President, 2002), the 107th U.S. Congress established the Department of Homeland Security in the Homeland Security Act of 2002 (PL 107-296, codified at 6 *USC* 111) on November 25 of that year. Section 101 of the Act specifies the mission of the Department, and the first four of the six elements that identify its "primary mission" focus on terrorism: (1) to "prevent terrorist attacks within the United States," (2) to "reduce the vulnerability of the United States to terrorism," (3) to "minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States," and (4) to "carry out all functions of entities transferred to the Department, including by acting as a focal point regarding natural and manmade crises and emergency planning."

As recounted by Brown and Cox (2011) and others, Congress "urged DHS to work with" U.S. national laboratories, particularly those in the Department of Energy, to identify and assess "newly recognized risks." The labs identified probabilistic risk assessment (PRA) as the primary means to do so, the major technique used to identify and assess risks related to nuclear accidents (pp. 202–203). PRA was initially developed at AT&T's Bell Labs in the early 1960s to address questions related to missile defense and launch, then Boeing Labs in the mid-1960s adapted the technique to determine planes' performance and reliability, and only then did the nuclear power community adapt PRA to assess nuclear reactors' safety, beginning in the 1970s (National Research Council, 2008, p. 112). The 2002 Act also specified risk management principles, especially for coordination of critical infrastructure protection (U.S. GAO, 2009, p. 6).

2.1. Probabilistic risk assessment (PRA)

Risk analysis according to PRA depends upon methods such as event trees, fault trees, and other means to make probability assessments. Under this concept, "management" of risk is said to involve three essential variables: threat, vulnerability, and consequence. These are commonly acronymized to TVC and have been the means by which the Department of Homeland Security has audited the performance and allocation of resources to protect the nation by the Department's component parts (e.g., RAND, 2012; U.S. Congressional Research Service, 2007; U.S. Government Accountability Office, 2009).

Thus, probabilistic risk assessment is an engineering technique that has come to dominate U.S. anti-terrorist efforts. Michael Chertoff, the second secretary of DHS (2005–2009), was especially influential in committing the Department and its many component parts to PRA as a primary means to protect national security, from his Senate confirmation hearing through his entire tenure as secretary (U.S. Congressional Research Service, 2007, pp. 1ff.). The use of PRA is a distinguishing characteristic particularly of anti-terror initiatives in international and domestic air travel as explored more fully below. Christine Wormuth, then Senior Fellow at the International Security Program at the Center for Strategic and International Studies, testified before the House Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Committee on Homeland Security in 2005 strongly asserting that the TVC model for risk assessment is "at the heart of the DHS approach" to security, most especially in transportation. She described how the Department has used the technique for planning, resource allocation, and policy development overall. Further, TVC should have played, in her opinion, the lead role in developing a National Security Risk Assessment as per the DHS enabling legislation. Probabilistic risk assessment as a whole, the triadic threat–vulnerability–consequence formula, and risk management more generally have been the subject of considerable critique on grounds ranging from the theoretical, the mathematical, the ideological, and beyond. A brief example of such a critique of the foundations of PRA might be useful here.

A more general formula for expressing risk is: $R = P \times C$, where R = risk, P = probability, and C = consequence. Of course, for acts of terror, we cannot determine P, nor can we determine C's many elements (e.g., Wormuth, 2005, p. 3); this is the essential paradox of un-knowing at the heart of risk assessment. This un-knowing both results from and is an expression of the fact that, for example, airline safety programs, such as the Automated Targeting System at the Department of Homeland Security, try to identify "terrorists who are not (yet) terrorists," fulfilling a "desire for preemptive identification and disruption" (Amoore & de Goede, 2008, p. 8).

Additional elements in risk assessment include the adoption of data mining as a key component (e.g., Seifert, 2004) and the use of scenario planning and testing, disaster rehearsal, link analysis, and similar techniques to complement the algorithmic approach of sophisticated PRA (e.g., Amoore & de Goede, 2008, p. 11). Despite the many critiques of PRA, it would be patently unfair and inaccurate to characterize the adopters and utilizers of risk management and risk assessment (including probabilistic risk assessment) in the security apparatus of the United States and elsewhere as naïve. Wormuth (2005, p. 3), for example, says that, We can create quite sophisticated "representations of probability and consequences, but they will be just that — representations rather than certainties." Those representations are only "descriptors not predictors."

The Transportation Security Administration uses risk assessment as the primary guide for its security decisions. What follows is a brief discussion of this usage, followed by a consideration of the *futurized imaginary* fueled by security risk assessments.

2.2. Risk assessment in the Transportation Security Administration

While responsibility for transportation safety is an element of almost all parts of the complex DHS organization, it is the Transportation Security Administration (TSA) that is especially given the task of protecting air transportation, including passengers, cargo, airports, air crews, aircraft, and so on; it also concerns itself with rail, highway, pipeline, and transit system safety. As stated explicitly on the TSA About page, "TSA employs a risk-based strategy," and this strategy is especially important to securing air transport. TSA must balance many competing and, at times, incompatible interests, beyond the risk of terror itself, such as costs for airlines and other carriers, implementation and maintenance costs of particular policy decisions, and burdens on travelers related to privacy, time lost, and the like (RAND, 2012, p. 123.) Information about the risk-based strategy used by TSA, including ATS, is rarely available publicly because of concerns with security. Whether that rationale can withstand scrutiny, however, is an open question, especially if legislators, judges, and domain experts should review the full panoply of TSA and other Homeland Security risk assessment practices. Such questions are among the most important rationales for some of the recommendations at the conclusion of this paper. Despite the surrounding secrecy, two additional documents, however, provide important insight into TSA's full embrace of risk assessment, especially with regard to air transportation: a 2009 Government Accountability Office (GAO) report on *Transportation Security: Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocation* and a 2012 RAND report *Modeling Terrorism Risk to the Air Transportation System: An Independent Assessment of TSA's Risk Management Analysis Tool and Associated Methods*, prepared for the TSA by RAND's Homeland Security and Defense Center.