H-Diplo | ISSF

Review Essay 42

Matthew Bunn and Scott D. Sagan (eds.) *Insider Threats*. Ithaca and London: Cornell University Press, 2016. ISBN: 9781501705168 (paperback, $22.95).

Reviewed by **Philipp C. Bleek**, Middlebury Institute of International Studies at Monterey

Published **5 October 2018** | issforum.org

Review Editors: **James Lebovic and Diane Labrosse**
Web and Production Editor: **George Fujii**

Shortlink: http://tiny.cc/ISSF-RE42
Permalink: https://issforum.org/essays/42-insider
PDF URL: https://issforum.org/ISSF/PDF/RE42.pdf

Red Flags Waving in the Wind: Insider Threats and What to Do (and Not Do) About Them

The possibility that terrorists might detonate nuclear fission bombs has seized both the general public and policy communities' attention since the September 11, 2001 terrorist attacks. Experts differ significantly on how likely or even plausible the threat might be, with well-informed, thoughtful analysts adopting views across the spectrum. Even among these diverging views, there is a relative consensus that terrorists are not likely to develop their own fissile material for nuclear weapons, and also that building even a crude nuclear device would require considerable expertise. Those working inside military, government, or commercial establishments may provide crucial materials or skills to terrorist groups who would otherwise be hampered in realizing nuclear attack motivations. More generally, insiders have the potential to pose significant nuclear threats. For example, causing a consequential radiation release from a nuclear reactor via external attack is challenging, but far less so with an insider accomplice.

The nuclear threats that insiders pose motivated the work that grew into Matthew Bunn and Scott Sagan's co-edited *Insider Threats*, though much of the book's content is also relevant to assessing and countering threats outside the nuclear domain. As the authors observe, "in a world of nuclear weapons, deadly pathogens, potentially devastating cyber intrusions, and high-capability terrorist groups bent on mass destruction, the stakes in dealing with insiders have never been higher" (5).

Sagan and Bunn are two of the most influential producers of rigorous, policy-relevant analysis of nuclear threats and responses. Sagan is an academic who orients his work around essential policy challenges, Bunn is a policy analyst who has found a home in academia. They are exceptionally well-

suited to shepherding this particular project. In the interests of full disclosure, both have also generously supported my own professional trajectory, so I am far from a disinterested observer.

As Bunn and Sagan observe in framing the book, even elite national security organizations have troubling track records regarding insider threats. They describe the surprising complacency that can emerge when organizational and cognitive biases—a major theme of Sagan's scholarship on nuclear dangers[1]—lead managers to downplay potential threats. In retrospect, the most troubling insider threats are often characterized by remarkable patterns of warning signs that were not observed and/or not heeded. As Sagan and Bunn evocatively observe, "Red flags are often waving in the wind, but no one sees them" (3).

Part of the problem, they diagnose, is that those responsible for security often have only limited information about incidents and best practices in other organizations. They observe that "While in the field of safety, sharing of information about accidents and lessons learned is routine, and there are regularized processes for it, in the field of security, with its penumbra of secrecy and its (often legitimate) fear of external enemies, little such sharing takes place…" (145-146). Bunn and Sagan intend this book to be a modest step toward remedying that, both in its own right and by catalyzing additional work on the topic.

The book blends an eclectic set of content, authored by a diverse, top-notch set of contributors, that works as a coherent whole. Chapters address the magnitude of terrorist threats to nuclear facilities, a post-mortem on the 2009 Ft. Hood shootings, another on the 2001 Amerithrax letters, analysis of the 2011-12 surge and then 2013 decline of "green-on-blue" attacks by Afghan soldiers on international coalition soldiers, and case studies on countering insider threats in the casino and pharmaceutical industries. Bunn and Sagan tie it all together with a "worst-practices guide" on how *not* to address insider threats.

Thomas Hegghammer, a leading scholar of jihadi terrorism, and Andreas Hoelstad Daehli, previously his research assistant, grapple with the magnitude of terrorist threats to nuclear facilities.[2] Unlike much writing on the topic which is more conceptual or focuses on single case studies, the authors built a data set of nuclear incidents and delved deeply into terrorist writings to explore potential motivations. The bottom line leaves room for guarded optimism. Although there have been many insider incidents at nuclear facilities, only a small fraction of them can be linked to

[1] See, among numerous relevant publications, Scott D. Sagan, *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons* (Princeton: Princeton University Press, 1995); Edward D. Blandford and Scott D. Sagan (eds.), *Learning from a Disaster: Improving Nuclear Safety and Security After Fukushima* (Stanford: Stanford University Press, 2016); Scott D. Sagan, "The Problem of Redundancy Problem: Why More Nuclear Security Forces May Produce Less Nuclear Security," *Risk Analysis* 24:4 (August 2004): 935-946.

[2] Thomas Hegghammer, and Andreas Hoelstad Daehli, "Insiders and Outsiders: A Survey of Terrorist Threats to Nuclear Facilities" in Matthew Bunn and Scott D. Sagan (eds.), *Insider Threats* (Ithaca and London: Cornell University Press, 2016).

terrorism motivations. That assessment is caveated by the fact that information in the public domain is almost certainly incomplete, and especially sparse as it relates to some key countries like Russia and Pakistan. Also hearteningly, the authors find little discussion of attacking nuclear facilities in the jihadi and far-right literatures—including online fora—in which they immersed themselves.

But there does appear to be *some* interest. One puzzle the authors observe is that terrorists interested in attacking nuclear facilities have given surprisingly little attention to insiders, despite the fact that "some of the literature suggests that insiders are such a force multiplier that infiltration should be the natural tactical choice of all prospective terrorists" (38-39). The authors speculate that perhaps "insider recruitment is too costly compared with other available tactics" (39). That seems plausible as far as it goes, but it also seems likely that those mulling attacking nuclear facilities in online chat rooms and elsewhere are mostly incapable and ill-informed. We are fortunate that chemical, biological, radiological, and nuclear (CBRN) terrorism broadly—and nuclear and radiological terrorism in particular—attract many actors who range from merely overconfident to delusional, and such actors are likely to overestimate their own capabilities and undermine even what limited capabilities they do have.[3] Of course, even a small fraction of more capable actors could wreak significant havoc, and even less capable actors may get lucky or their mostly or wholly failed plots might still have significant consequences.[4]

Amy Zegart, one of Sagan's faculty colleagues at Stanford who has done incisive work on the U.S. intelligence community, contributes a post-mortem on the 2009 Ft. Hood shootings.[5] Self-radicalized terrorist Major Nidal Malik Hassan killed thirteen of his fellow soldiers and injured far more. In retrospect, a striking pattern of red flags was missed or inadequately addressed. Remarkably, as Zegart chronicles, "Hasan was openly radical and flagrantly incompetent, defending Osama bin Laden, justifying suicide bombers, and declaring his devotion to Sharia law over the U.S. Constitution to his peers and supervisors in conversations, classes, and PowerPoint presentations over a period of years—all while barely fulfilling the requirements of his job" (42-43). Hassan was on

[3] Two actors toward the delusional end of the spectrum are the Japanese Aum Shinrikyo cult and Glendon Scott Crawford, a right-wing extremist. Aum Shinrikyo had limited success with chemical weapons, failed abjectly with biological weapons, had a minor and delusional nuclear weapons program, and pursued even more delusional attack modes including earthquake generators. Glendon Scott Crawford, a self-described Ku Klux Klan member, is in prison for plotting to covertly use a truck-borne industrial X-ray machine to irradiate Muslims. On Aum Shinrikyo, see Philipp C. Bleek, "Revisiting Aum Shinrikyo: New Insights into the Most Extensive Non-State Biological Weapons Program to Date" Analysis Paper, Nuclear Threat Initiative (December 2011). On Crawford, see Kristine Phillips, "A KKK member plotted to kill Muslims—with a homemade death ray" *Washington Post* (19 December 2016).

[4] These themes are elaborated in Zachary Kallenborn and Philipp C. Bleek, "Avatars of the Earth: Radical Environmentalism and Chemical, Biological, Radiological, and Nuclear (CBRN) Terrorism," *Studies in Conflict & Terrorism* (May 2018).

[5] Amy B. Zegart, "The Fort Hood Terrorist Attack: An Organizational Postmortem of Army and FBI Deficiencies" in Matthew Bunn and Scott D. Sagan (eds.), *Insider Threats* (Ithaca and London: Cornell University Press, 2016).

the FBI's radar starting a year before the attack because of emails he exchanged with a Yemen-based U.S. cleric notorious for inspiring terrorism. And all of this occurred in the years after the 9/11 terrorism attacks, when awareness of such dangers was high and various reforms had been enacted to better address them.

Contra existing scholarship, Zegart argues that "Policies, people, and political correctness are important parts of the story, but they are not the most important parts" (44). Instead, she blames a combination of misplaced incentives and miscommunication between organizations, arguing that "the insider attack occurred less because individuals screwed up than because both organizations [the Army and the FBI] were poorly adapted to prevent it" (71). As organizations in the national security domain become ever more complex, mitigating the pathologies that Zegart highlights—both here and in her other work[6]—is likely to become ever more challenging.

Jessica Stern, an influential terrorism analyst, and Ronald Schouten, a psychiatrist with professional interests that include terrorist psychology, profile Bruce Ivins, widely accepted to have been the perpetrator behind the 2001 Amerithrax letters, killing five, infecting seventeen, and affecting many others in various ways.[7] Like Zegart, the authors chronicle what in retrospect is an appalling collection of red flags. As they summarize, "While viewed at the laboratory [where he worked, the U.S. Army Medical Research Institute of Infectious Disease] as able and likable, if eccentric, Ivins in fact had a long and troubling history of mental illness, substance abuse, obsession with a sorority and its members, homicidal thoughts, and criminal acts (including theft, vandalism, trespass, and breaking and entering)" (75).

The authors blame "a complicated mix of evolving regulations, organizational culture, red flags ignored, and happenstance" (75). Perhaps most troublingly, the authors observe that "some of the same organizational failures that came to light as a result of the anthrax letter mailings played a role in the series of biosecurity and safety failures at high-containment labs disclosed in 2014" (102). The authors pessimistically conclude that "We expect future 'predictable surprises' as a result" (102).

Austin Long, whose work incisively addresses a broad range of international security issues, explores the 2011-12 surge and then 2013 decline of "green-on-blue" attacks by Afghan soldiers on international coalition soldiers.[8] As Long describes, a decade after a U.S.-led coalition entered

[6] Among other publications, see Amy Zegart, *Spying Blind: The CIA, the FBI, and the Origins of 9/11* (Princeton: Princeton University Press, 2009).

[7] Jessica Stern and Ronald Schouten, "Lessons from the Anthrax Letters" in Matthew Bunn and Scott D. Sagan (eds.), *Insider Threats* (Ithaca and London: Cornell University Press, 2016).

[8] Austin Long, "Green-on-Blue Violence: A First Look at Lessons from the Insider Threat in Afghanistan" in Matthew Bunn and Scott D. Sagan (eds.), *Insider Threats* (Ithaca and London: Cornell University Press, 2016).

Afghanistan in 2001, between January 2011 and December 2012 the rate of insider attacks spiked dramatically. Then it plummeted just as dramatically in 2013.

In examining the motivations of those perpetrating attacks, Long proposes an analog to Albert O. Hirshman's classic framing of the options facing those dissatisfied with an organization, *Exit, Voice, and Loyalty*.[9] Long argues that dissatisfied Afghan soldiers could exit (desertion), act violently (as a means of exercising voice), and be disloyal (remaining in the unit but aiding the enemy). Long also argues that individual rage could trump strategic choices. Examining the empirics, he postulates that the insurgency may have observed the success of insider attacks and chosen to promote them more in 2011 and 2012. Long also suggests that personal motivations, especially rage, are crucial explanations. He explores the nuances of the particular ideological, cultural, and tribal contexts in which these behaviors emerged.

As for the rapid decline in attacks in 2013, Long gives significant credit to a combination of proactive and defensive measures implemented by military officials who saw insider attacks as posing severe threats, especially to coalition cohesion. Long's bottom line is that under some conditions novel threats may emerge quickly, but also that it may be feasible to quickly ameliorate them. The case study is fascinating, even if the evidence available to assess it is more suggestive than definitive, and even if it seems more tenuously relevant to the book's core themes than the other chapters.

Bunn and Kathryn M. Glynn, a Harvard Kennedy School masters student who wrote a related thesis, examine how the casino and pharmaceutical industries counter insider threats.[10] Both industries have profit incentives to find effective ways to guard against insider threats, hence plausibly offer lessons for facilities that store nuclear material (as well as other sensitive facilities). As one might expect, the authors find that many of the general approaches taken in these two industries are already mirrored in the security practices of nuclear facilities in various countries.

One intriguing insight is that "To address the possibility of the casino's general manager being involved in activities that he or she might wish to cover up, the surveillance team reports to a distinct chain of command…" (129). According to the authors, while casinos have chosen to stovepipe surveillance, pharmaceutical plants instead integrate it into broader security activities. Both approaches seem viable, with pros and cons, when it comes to nuclear material security (and other domains).

[9] Albert O. Hirshmann, *Exit, Voice, Loyalty: Responses to Decline in Firms, Organizations, and States* (Cambridge: Harvard University Press, 1972).

[10] Matthew Bunn and Kathryn M. Glynn, "Preventing Insider Theft: Lessons from the Casino and Pharmaceutical Industries" in Matthew Bunn and Scott D. Sagan (eds.), *Insider Threats* (Ithaca and London: Cornell University Press, 2016).

Yet the authors also argue that context and objectives differ in important ways between these industries and facilities where nuclear weapons-usable materials are secured. Most fundamentally, they find that "both [casino and pharmaceutical] industries accept that in some cases the expense of preventing small thefts may not be worth the cost of prevention—attitudes those handling weapons-usable nuclear material cannot afford to adopt when it comes to kilogram quantities…" (123).[11]

Bunn and Sagan tie it all together with a "worst-practices guide" on how *not* to address insider threats.[12] The chapter is a must-read for anyone motivated to ameliorate insider threats; the pearls of wisdom it offers are too numerous to do them justice by trying to succinctly summarize them here. Anyone who has worked on national security issues in the U.S. government—and presumably many who work elsewhere—will recognize many of the pathologies they highlight.

Even organizations deeply invested in national security sometimes act in ways that are remarkably ill-considered. A simple example—albeit not one directly related to insider threats—comes to mind from my own time serving as a civilian in the U.S. Office of the Secretary of Defense, where among other activities I staffed a Pentagon-based, interagency group focused on Syrian chemical weapons.[13] My colleagues and I regularly commuted by subway from the Pentagon to meetings at the White House. Following regulations, we would courier classified documents in brightly colored, intrusion-resistant, locked pouches that were both visually distinctive and too large and rigid to fit into a standard briefcase. Openly carrying those distinctive pouches in public felt like we had "steal me" signs on us. It is hard to fathom a good reason for not making those pouches look more generic and/or be able to be concealed inside a briefcase. And yet for years U.S. government employees have been carrying around sensitive secrets that way. Perhaps someone sufficiently influential will read this and a company will win a lucrative contract to manufacture better pouches?

Bunn and Sagan close with an important cautionary note. Their book highlights multiple examples of missed red flags. But it is also important not to see red flags where there are none, which can impair organizational effectiveness, including efforts to discern and respond to legitimate threats.

Policymakers face tremendous pressures to pursue illusory perfect security, rather than recognizing that security will always be inherently imperfect and instead balancing competing interests. Bunn, Sagan, and all their other contributors offer thought-provoking generalizations and informative real-

[11] Then again, kilogram quantities of pharmaceuticals or of casino chips or cash are unlikely to be so cavalierly seen by those industries. But their point that losses of nuclear material are potentially far more consequential than similarly-sized losses of pharmaceuticals or cash is well taken.

[12] Matthew Bunn and Scott D. Sagan, "A Worst Practices Guide to Insider Threats" in Matthew Bunn and Scott D. Sagan (eds.), *Insider Threats* (Ithaca and London: Cornell University Press, 2016).

[13] Philipp C. Bleek and Nicholas J. Kramer, "Eliminating Syria's Chemical Weapons and Implications for Addressing Nuclear, Biological, and Chemical Threats Elsewhere," *Nonproliferation Review* 23:1 (2016): 197-230.

world case information; effectively implementing insights gleaned will necessarily be deeply context-dependent.

Philipp C. Bleek is Associate Professor and Program Chair (Acting) in the Nonproliferation and Terrorism Studies program at the Middlebury Institute of International Studies at Monterey. He works on the causes, consequences, and amelioration of chemical, biological, radiological, and nuclear weapons threats at the intersection of academia, non-governmental organizations, and government. His most recent publication is "Avatars of the Earth: Radical Environmentalism and Chemical, Biological, Radiological, and Nuclear (CBRN) Terrorism," (with Zachary Kallenborn), *Studies in Conflict & Terrorism* (May 2018).