HARVARD Kennedy School
BELFER CENTER
FOR SCIENCE AND INTERNATIONAL AFFAIRS

Violent extremism and insider threats – what should nuclear organizations do?

Matthew Bunn
James R. Schlesinger Professor of the Practice of Energy, National Security, and Foreign Policy, Harvard Kennedy School

International Nuclear Security Forum

24 March 2021

belfercenter.org/managingtheatom

1

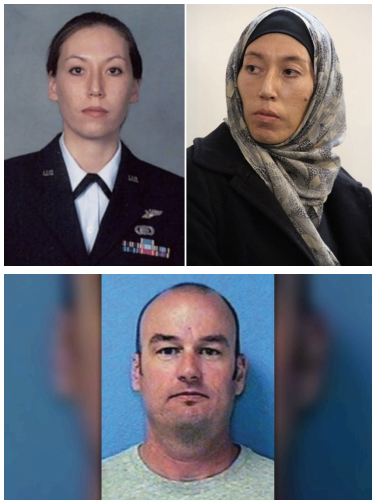
Coping with Violent Political Extremism and Insider Threats is a Major Challenge

- Recent events demonstrate that the risk of violent extremists at nuclear facilities is very real
- In the United States (and many other countries), people have freedom of ideas, association
- Need to carefully balance:
  - Political freedom
  - Successful operations
  - Mitigating insider threats
  - Safety, other elements of security, other objectives…
- Existing U.S. programs – such as the Human Reliability Program – are critical
  - But not mainly designed to address domestic violent extremists
- U.S. military working to address the issue – private companies, contractors, have fewer tools

2

Pre-1/6 U.S. Examples: Insiders Charged with Spying, Preparing to Kill

- February 2019: Monica Witt (Fatemah Zarah), indicted for spying for Iran
  - 10-yr Air Force intelligence veteran (and later contractor)
  - Allegedly helped target U.S. agents, revealed a SIGINT program
  - Defected to Iran in 2013
- February 2019: Lt. Christopher Hasson, arrested, charged with plotting domestic terrorism
  - >20 yrs in Coast Guard
  - Allegedly planned to kill leading left-leaning political, media figures
  - 2017 letter: "dreaming of a way to kill almost every last person"
  - Insider position apparently not used



Monica Witt, Christopher Hasson
Source: U.S. Justice Department

3

A Recent Nuclear Example: Insider Sabotage and a Cleared Terrorist at Doel-4

- August 2014: An insider at Doel-4 reactor in Belgium drains lubricant, destroys reactor turbine
  - ~$200 million damage
  - Investigators unable to find culprit
  - Sabotage not intended to cause radiation release
- Long before, Ilyass Boughalab had access to vital area
  - Passed security clearance review in 2009
  - In late 2012, he and another employee left to fight for terrorists in Syria (Boughalab killed there)
  - Later convicted as part of "Sharia4Belgium" terrorist group

Ilyass Boughalab
Source: Kristof Pieters

4

Cognitive, Organizational Biases Undermine our Ability to Cope with Insider Threats

- Insiders are trusted, authorized employees
  - Other employees see them as friends, colleagues
- Cognitive dissonance, affect bias, illusion of control lead people to ignore warning signs
  - Even more challenging when signs are legitimate political statements
- Organizational dysfunction adds disincentives to reporting, acting on warning indicators
- Even seemingly obvious "red flags" are sometimes ignored

Doel-4 nuclear power plant – sabotaged by an insider in 2014

5

5

Nuclear Organizations Cannot Rely on Any Single Security Measure Against Insiders

- Insiders are embedded in the organization for months or years, can plan ways to overcome security measures
- Cannot rely <u>only</u> on:
  - Background checks
  - Human reliability, monitoring programs
  - Two-person rule
  - Rules limiting access to certain areas, materials
- Need multiple measures working in concert

Beant Singh and Indira Gandhi

6

6

Insider threats: What should organizations do?

- Build high-performance and high-vigilance culture – everyone understands that security is their job too
- Build a comprehensive, multi-layered approach to reducing insider threats
  - Maximize the scale and complexity of challenges insider adversaries would have to overcome
- Include regular assessment, testing, "red teaming" as a key part of the insider program
- Design approach within the context of the laws, culture of your country and organization
  - Need to balance maintaining vigilance with fostering atmosphere of trust, cooperation needed for high performance

7

7

Insider threats: What should organizations do? (II)

- A comprehensive approach should include:
  - Thorough background checks before access
  - Ongoing monitoring of behavior
  - Requirements, incentives to report both concerning behavior and potential vulnerabilities
  - Effective training – with real stories
  - Minimizing human access to vital areas, materials, information
  - Continuously monitoring, controlling, and accounting for vital areas, materials, information
  - Effective investigations, responses to reports – seen as fair and reasonable by staff

8

8

A Worst Practices Guide to Preventing Leaks, Attacks, Theft, and Sabotage

http://www.belfercenter.org/publication/insider-threats

9