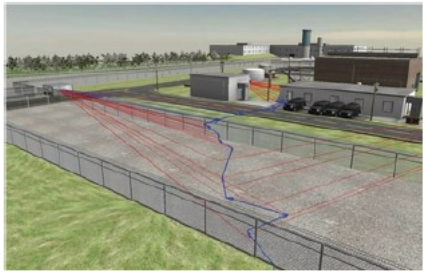
HARVARD Kennedy School
BELFER CENTER
FOR SCIENCE AND INTERNATIONAL AFFAIRS

Modeling of nuclear security: Use the tool, but remember its limits

Matthew Bunn
Professor of Practice, Harvard Kennedy School
"Emerging Issues in Nuclear Security," INMM/Managing the Atom
5 August 2019
belfercenter.org/managingtheatom

Modeling and simulation: a crucial tool for evaluating nuclear security systems

- In-depth simulation allows
  - Exploration, visualization of wide range of scenarios
  - Assessment of different defense designs, tactics
- Used with exercises, can assess performance better than with testing plus force-on-force alone
- Can help find ways to get more effectiveness for less money, inconvenience
- But, modeling and simulation is only a tool
  - Simulation results are only part of an effectiveness evaluation
  - Need to be aware of the strengths and weaknesses of the tool



Source: ARES Corp.

Challenge 1: Large unknowns

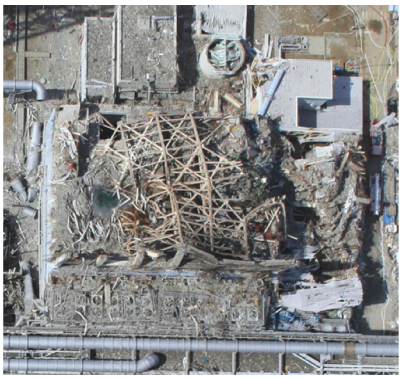
3

- Always a challenge collecting good data to use in modeling
- But we don't really know:
  - What numbers, capabilities, tactics the adversary will use
  - What system weaknesses they will try to exploit
  - How the guard force will react in the moment
  - What the full scope of consequences might be
  - …
- What questions are we not asking that will seem obvious after an incident?

Challenge 2:
We can only model what we think of

4

- In major heists from guarded facilities, security systems are usually defeated by means the defenders didn't plan for
- TMI, Chernobyl accident sequences had never appeared on any PRA – Fukushima sequence dismissed as too low-probability to worry about
- No substitute for creative people with a "hacker" mentality thinking about how to defeat defenses
  - Need organization's support – not ostracism when they find problems



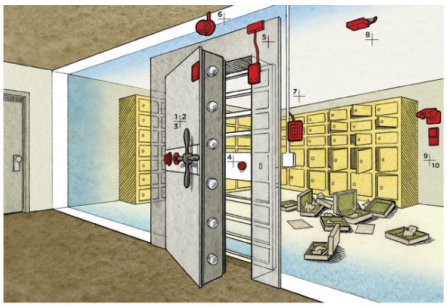
Source: Air Photo Service, Japan

Challenge 2: (II)
We can only model what we think of

5

"Infinity Maxim: There are an unlimited number of security vulnerabilities for a given security device, system, or program, most of which will never be discovered (by the good guys or bad guys)."

-- Roger Johnston, *Security Maxims*



The Door
1. Combination dial (0-99)
2. Keyed lock
3. Seismic sensor (built-in)
4. Locked steel grate
5. Magnetic sensor
6. External security camera

The Vault
7. Keypad for disarming sensors
8. Light sensor
9. Internal security camera
10. Heat/motion sensor (approximate location)

Defenses defeated in the Antwerp Diamond Center heist, 2003
Source: *Wired*

Challenge 3:
Complexity and tight coupling

6

- Complexity: Behavior of the system is different from the sum of the parts – difficult to predict
  - E.g., false alarm rates or contract structure may affect guard behavior
- Tight coupling: Action in one part of the system propagates to other parts faster than people can respond
  - Once incident begins, events sometimes unfold at high speed
- Partial solutions:
  - Simple systems
  - Redundant systems
  - More delay to loosen coupling

Challenge 4: Modeling human, organizational behavior

7

- "Good security is 20% equipment and 80% culture"
  - Gen. Eugene Habiger
- What the rules and procedures say people should do is often very different from what happens day-to-day
  - What assumptions in our models about what the people do will prove to be valid?
  - How can we incorporate possible weaknesses arising from organizational dysfunction, misdirected incentives…?
  - Are we just modeling the 20%?

Graffiti from Y-12 break-in

Importance of the "human factor"

- *Intelligent adversaries* will seek to identify and exploit weaknesses in the system
  - Will actively try to think of things the security planners *haven't* thought of
  - Insiders are particularly difficult to model, and to protect against: they know the system and its weaknesses (may be among the vulnerability assessors), are trusted by other employees
- *Intelligent employees* will seek to avoid doing things that are inconvenient, boring, that they perceive as unimportant, and that distract from other activities more likely to bring promotion, raises, or pleasure
  - Guards will say they patrolled, checked locks, when they didn't – when the Superbowl is on, they may be watching TV, not the fences
  - Personnel in general will disregard security rules they think are excessive or useless, and will not behave in the way that system designers may expect – has to be taken into account

Challenge 5: Complexities of insider threats

10

- Insiders have months or years to observe security practices, develop plans to defeat them
  - Potentially far more than the effort that will be put into a vulnerability assessment
- Insiders may arrange to disable security features that are key to system performance in our models
- Key insider protections – such as high employee morale, effective reporting systems – are difficult to model
- Cognitive, organizational biases tend to blind organizations to insider threats

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

Challenge 6: Distracting us from the unmodeled

11

- "What you see is all there is" (WYSIATI)
  - Models focus our thinking on what's in the model
  - Tend to forget to think about what might NOT be in the model
  - Tend to assume the world works as the model does
  - "Theory-induced blindness"
- Classic experiment (Fischhoff, Slovic, Lichtenstein, 1978):
  - Shown a fault tree, people assumed it covered all but a small (roughly constant) fraction of possible causes of a car not starting, *regardless of what fraction were actually included*
  - Was true even of trained mechanics
- Focus on violent outsider attack could lead us to think less about possibly more likely threats:
  - Insider threats (including >1 insider – common in heists)
  - Deception threats (e.g., fake uniforms, IDs, paperwork…)
  - Stealth
  - Unusual routes in (e.g., tunnels, helicopters…)

Questions policymakers should ask about models on any topic

12

1. What assumptions most drive the outcome – and how valid are they?
2. How does the model do in reproducing the system's response to things that *have* happened?
3. Can the modeler explain *why* the model behaves as it does, and why the real world should do the same?
4. How do the results of this model compare with the results of other more or less independent models?
5. How well do the *pieces* of the model represent the real behavior of the real things they are modeling?

Questions policymakers should ask about models on any topic (II)

13

6. Does the model include key interactions that the policymaker can guess would occur in the real world?
7. Does the model include interactions and effects that do *not* seem to correspond to those in the real world?
8. Has the model and its results undergone peer review?
9. How do we know? What kind of evidence was used to build the model?
10. What's the uncertainty?

Some (very partial) solutions

14

- Use modeling and simulation – but only as one tool in the suite of ways to understand vulnerability, effectiveness
  - Remember the challenges and pitfalls
  - Continue force-on-force exercises, tabletops, small-group vulnerability explorations…
- Include teams of creative, "hacker" types in vulnerability assessments, with real incentives to find vulnerabilities
- Expand use of simple, "passively secure" systems
- Take steps to strengthen security culture, address organizational issues
- Design great models! (Realistic, validated, and easy to use, understand) – and use them carefully