HITTING THE 'SNOOZE' BUTTON ON NUCLEAR SECURITY:

Stuxnet and the Wake-Up Call It Should Have Been

Alexandra Van Dine
Program Associate, Scientific and Technical Affairs
Nuclear Threat Initiative
vandine@nti.org
(202)454-7758

NTI
BUILDING A SAFER WORLD

The risk of nuclear terrorism may be one of the gravest threats of our time

Cyber attacks could facilitate acts of nuclear theft or sabotage

Stuxnet: A Case Study

- Operation Olympic Games lasted from 2006 until 2010, though Stuxnet is still in the wild

- Precision cyber weapon targeted on Natanz, a hidden Iranian uranium enrichment facility
  - Part of a clandestine nuclear program
  - Air-gapped, geographically hidden

Why should we worry?

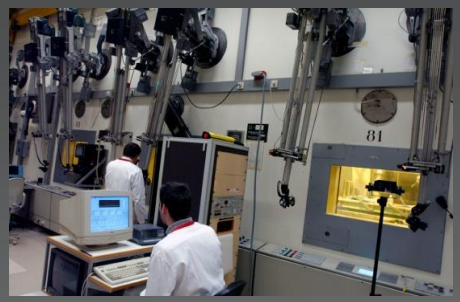
- Natanz: by any measure, a hard target
  - What happens when more accessible facilities, like power plants, are attacked?

- Stuxnet: precision weapon targeted on a specific facility with limited potential for radiation release
  - This will not necessarily be the case in future attacks

A variety of nuclear systems are vulnerable to cyber attacks with physical consequences

Power Generation
- Sabotage
- Radiation release

Physical Protection
- Theft
- Sabotage



Fuel Processing
- Theft
- Sabotage

Materials Accountancy
- Theft
- Diversion

Has Stuxnet motivated any reforms in facility security?

- Some recent movement on regulations
  - Not necessarily a product of Stuxnet
  - Implementation not yet adequate
  - Relevant areas not always covered (e.g. nuclear materials accounting)
- Facility security measures have not kept pace with the threat
  - Laptops, flash drives
  - Digital systems
  - Inadeqate security measures (e.g., firewalls, airgaps, antivirus)
  - Outdated safety analyses

What is slowing progress?

Complexity of Digital/Physical Systems

Compliance Mindset

Uneven Distribution of Limited Human Capacity

Bureaucratic Inertia

Cost

Bridging Technical/Policy Language Gap

How can we move forward?

- Re-examine existing principles and implement best practices for cyber at nuclear facilities
  - e.g., controlling laptop entry
- Consider implementing modern technical solutions
  - Revolutionary vs. evolutionary
- Work to address human capacity issue
  - Support IAEA training efforts
  - Explore options for a global cyber capability

Thank You!