PARTNERSHIP *for* GLOBAL SECURITY
LEADING THE WORLD TO A SAFER FUTURE

TECHNOLOGY IN THE 21ST CENTURY: CYBER AND AI CHALLENGES

NUCLEAR SECURITY AND EMERGING TECHNOLOGIES: THE IMPACT OF CYBER AND ARTIFICIAL INTELLIGENCE & SECURITY AGAINST EMP

MARCH 22, 2018

Kenneth Luongo
President, Partnership for Global Security

Hoam Faculty House
Seoul National University
Seoul, South Korea

PARTNERSHIP for GLOBAL SECURITY
LEADING THE WORLD TO A SAFER FUTURE

Disruptive Technologies in the 21st Century

- The McKinsey Global Institute identified 17 emerging disruptive technologies in 2013 that can transform life, business, and the global economy. All of them fit into 5 categories:
  - Cyber/Computing
  - Artificial Intelligence
  - Energy
  - Materials
  - Biology
- Technologies in each of these categories are advancing quickly and some are creating significant economic impact.
- They also have serious security implications – nationally and internationally.
- In democratic nations most of these technologies are controlled and being driven by the private sector.
- In authoritarian nations these technologies are being nurtured and controlled by the government.

Disruptive technologies at a glance:
Word cloud of report contents[1]

1 www.wordle.net; McKinsey Global Institute analysis.

PARTNERSHIP for GLOBAL SECURITY
LEADING THE WORLD TO A SAFER FUTURE

Global Rivalry: The Technology Race

- Increasingly technology supremacy is the key competition between advanced nations and geopolitical rivals.
- The winner of this race will have significant impact on global security, economic growth and the international hierarchy.
- A major challenge is coming from China which seeks to dominate computing and artificial intelligence, among other advanced technologies.
- These technologies have significant intersections with nuclear energy (including advanced reactors) and global security.
- It matters who controls these technologies for the remainder of the century.
- The nuclear-cyber-AI intersection is critically important in NE Asia which will become the densest nuclear region in the 21st Century.

Cyber Challenges

PARTNERSHIP for GLOBAL SECURITY
LEADING THE WORLD TO A SAFER FUTURE

There are 5 Major challenges

1. Cyber attack
2. Cyber espionage
3. Cyber coercion
4. Cyber crime
5. Weaponization of social media and information

Cyberattacks

Exploitation of a security vulnerability through a connection to the Internet, such as:

- Malware (Trojans, viruses, and worms) – code that steals or destroys data. **Critical infrastructure control systems are facing advanced levels of malware.**
- Phishing – attack disguised as a request for data from a trusted 3rd party to steal information.
- Password attacks
- Denial-of service (DOS) attacks – attacks designed to disrupt a network's service resulting in the network unable to function.
- "Man in the Middle" – adversary impersonates the endpoints of an online exchange.
- Drive-by downloads – malware on a legitimate website that downloads itself to a user's system when the user simply visits the legitimate website.
- Malvertising – attack that uses malicious code to enter a user system after the user clicks on an ad that contains malicious code.
- Rogue software – malware that disguises itself as necessary security software.

Cyber-Nuclear Attacks: Some Cases

2003 – Slammer Worm infected computer systems at Davis-Besse nuclear plant in Ohio – worm travelled from a consultants network behind the reactor network's firewall.

2006 – Computer malfunction at Browns Ferry nuclear plant in Ohio caused failure of recirculation pumps (network problem not cyber attack but potential attack vector).

2008 – Software update at Hatch nuclear plant in Georgia caused automatic shutdown (not cyber attack but a possible attack vector).

2009 – Comanche Peak Nuclear Power Plant in Texas, insider malicious activity.

2010 – Stuxnet worm was a successful cyber attack against Iran's uranium enrichment infrastructure – government engineered worm.

2014 – KHNP computers hacked and information stolen – no reactors impacted.

2014 – Malware attack against (Japan's) Monju power plant Japan.

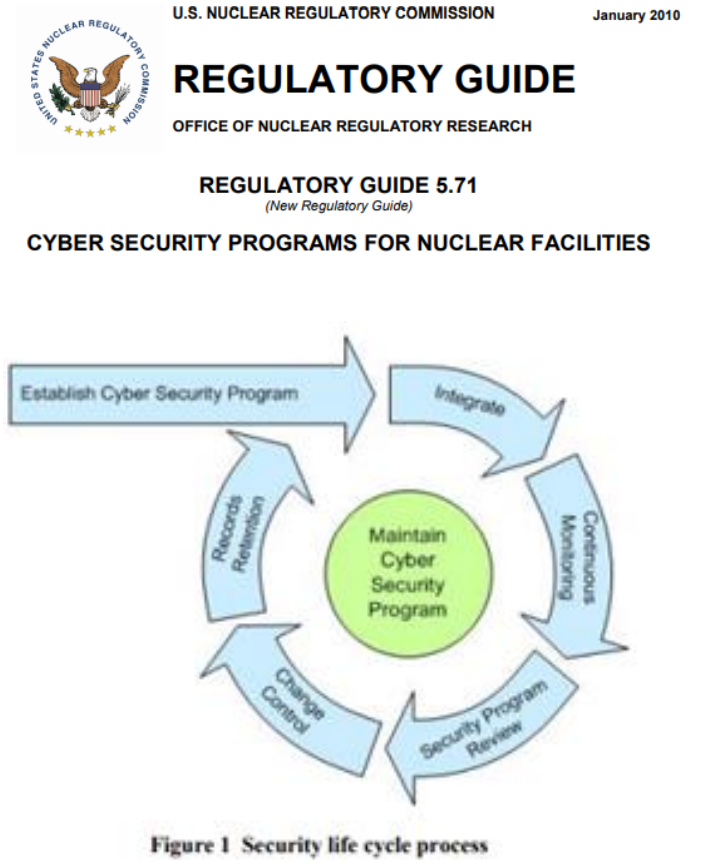
2017 – Wolf Creek Nuclear Operating Corp. (Kansas plant operator) targeted by hackers through Microsoft Word documents.

2015 – 2018 – Russian state hackers able to access the control systems of unnamed nuclear power plants.

No catastrophic damage to any reactor from attacks – YET.

NRC: Cyber Security Actions

- Initial NRC cyber security orders issues after 9/11; Final Rule finalized in March 2009; Regulatory Guide for Cyber Programs for Nuclear Facilities published January 2010.
- Regulations designed to protect reactor's digital systems - computer, communications and networks associated with safety and security functions, emergency preparedness, and support systems important for safety and security.
- Regulatory Guide includes "best practices" from International Society of Automation, Institute of Electrical and Electronics Engineers, National institute of Standards and Technology, Department of Homeland Security, and the Nuclear Energy Institute.
- NRC also considering cyber requirements for fuel cycle and spent fuel facilities, non-power reactors, decommissioned facilities, and materials.
- NRC established a Cyber Security Directorate in June 2013 for planning, coordination and management.


U.S. NUCLEAR REGULATORY COMMISSION January 2010

REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 5.71

(New Regulatory Guide)

CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES

Figure 1 Security life cycle process

Figure 1 illustrates the process of establishing, implementing, and maintaining the cyber security program.

Source: NRC Regulatory Guide 5.7.1

https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/cyber-security-bg.html

PARTNERSHIP for GLOBAL SECURITY
LEADING THE WORLD TO A SAFER FUTURE

Implementation of NRC Requirements

- Every company operating nuclear power plants has an NRC-approved cyber security program.
- Critical safety and security systems are isolated from the internet – no direct or indirect access to the web using either air gaps or hardware-based isolation devices – to protect against network-based cyber attacks originating outside the plant.
- Controls on portable media and equipment, incl. thumb drives, compact disks, and laptops – to protect against Stuxnet-like attack.
- Cyber training and increased security screening and behavioral observation to protect against insider threats.
- Periodic cyber security and vulnerability assessments and enhancement.

https://www.nei.org/resources/reports-briefs/cybersecurity-for-nuclear-power-plants

PARTNERSHIP for GLOBAL SECURITY
LEADING THE WORLD TO A SAFER FUTURE

Critical Analyses of Cyber Security Actions

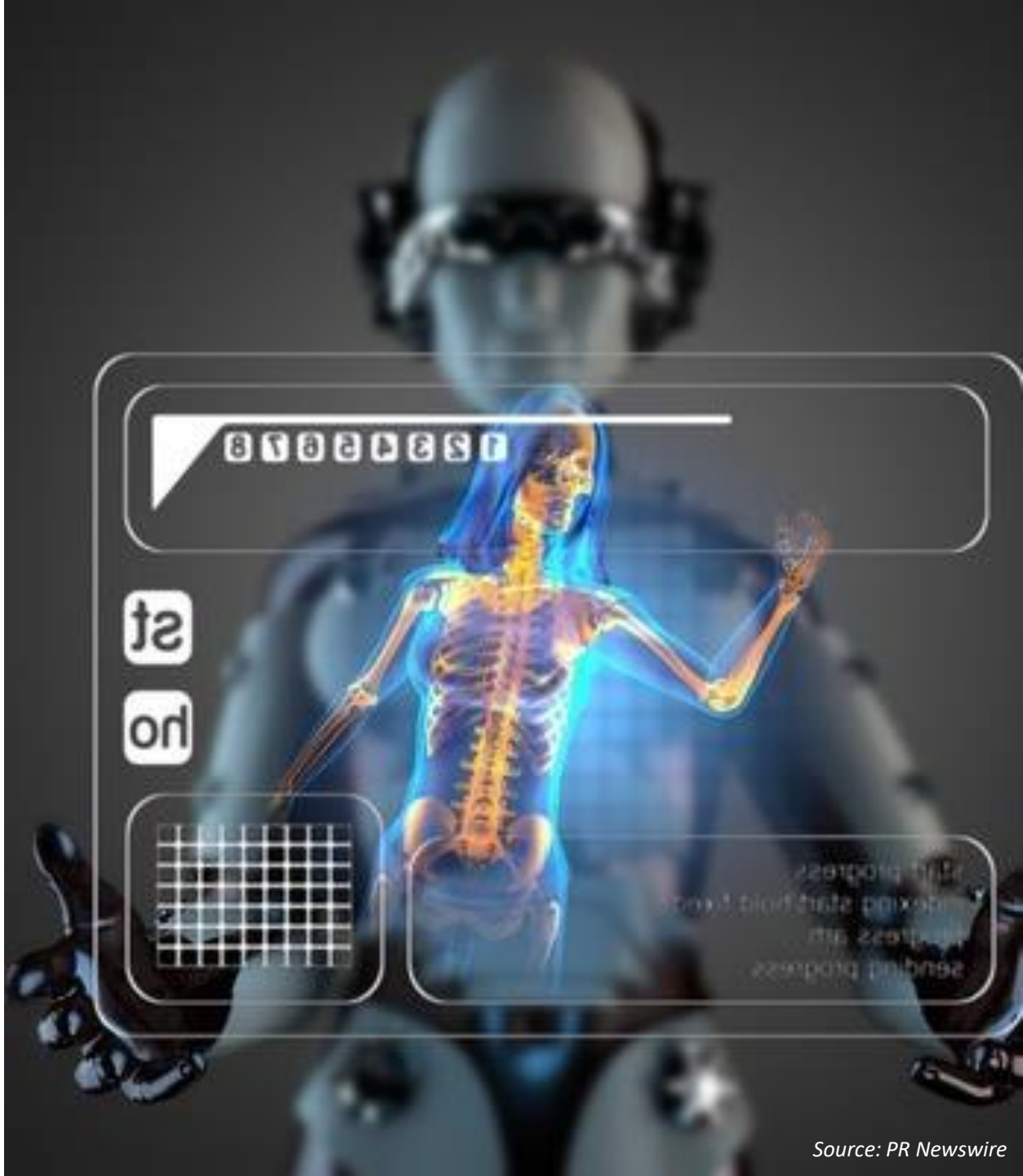
- Air gap "myth" – unintended network connections to isolated systems, malware on computer systems, human error, removable media.
- Limited collaboration and information sharing with other industries.
- Limitations of operator personnel understanding and training on cyber risks.
- Industrial controls that were not designed with cyber security in mind; need for transformative hard-to-hack technologies.
- Supply chain vulnerabilities outside reactor.
- Risks assessment is difficult to quantify; particularly acute for developing nations.
- Need for greater international dialogue and institutional support on cyber security.
- Requirement for active defenses, complexity reduction, more technical experts.

https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstoneUpdate.pdf
http://www.nti.org/media/documents/NTI_CyberThreats_FINAL.pdf

PARTNERSHIP for GLOBAL SECURITY
LEADING THE WORLD TO A SAFER FUTURE

AI Challenges

- Artificial Intelligence allows machines to exhibit human-like cognition.
- It is an explosive technology field rivaling computer chips in intensity of R&D.
- According to McKinsey& Co., in 2016, companies invested $26-39 billion, the vast majority by tech giants Facebook, Apple, Google and Twitter.
- By contrast, it is estimated that in 2015 the U.S. government spent $1.1. billion on unclassified AI R&D.
- There are many benefits from AI including robotics, healthcare, and high tech engineering.
- But there are significant challenges that need to be managed:
    - Potential Malicious or Unethical Programing
    - Potential Arms Race
    - Combination with Advanced Biotechnology
    - Lack of Governance Structure



Source: PR Newswire

AI-Nuclear Power-Security Interface

- AI is being used in the nuclear power field – nuclear equipment vendors, engineering firms, universities, national laboratories, and utilities.
- Some of the applications are power load predictions, training of personnel, reduction of reactor operator burdens, and power plant component inspection and fault detection.
- There is potential for "AI by design" in next generation advanced nuclear power plants.
- But, because this is a very intense research area, the full range of benefits and challenges for nuclear security are not yet fully explored.
- This workshop is designed to begin the dialogue on how artificial intelligence may help provide better nuclear security and how to develop governance regimes for managing its dangers.