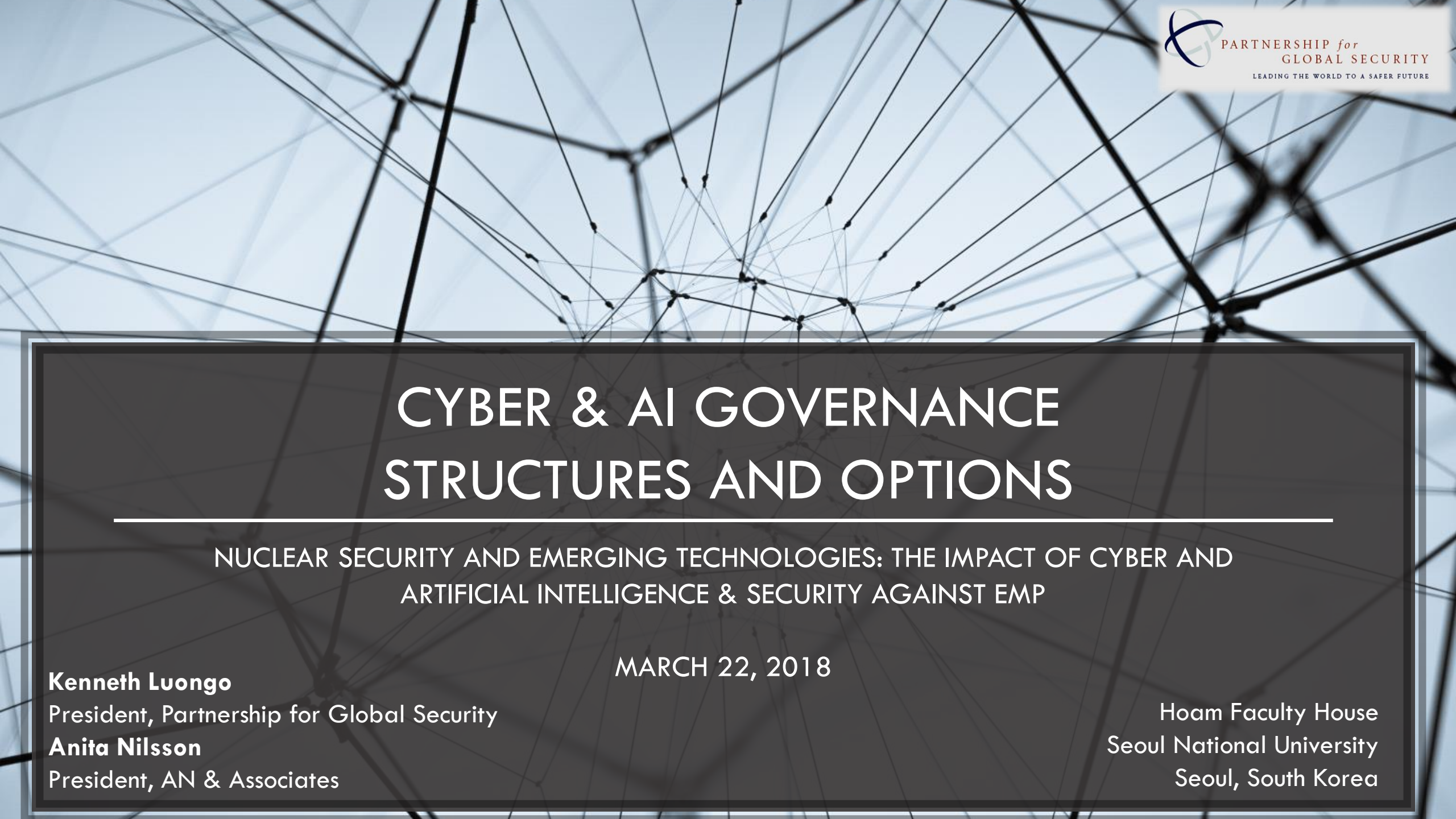


PARTNERSHIP for GLOBAL SECURITY
LEADING THE WORLD TO A SAFER FUTURE

CYBER & AI GOVERNANCE STRUCTURES AND OPTIONS

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
Anita Nilsson
President, AN & Associates

Hoam Faculty House
Seoul National University
Seoul, South Korea

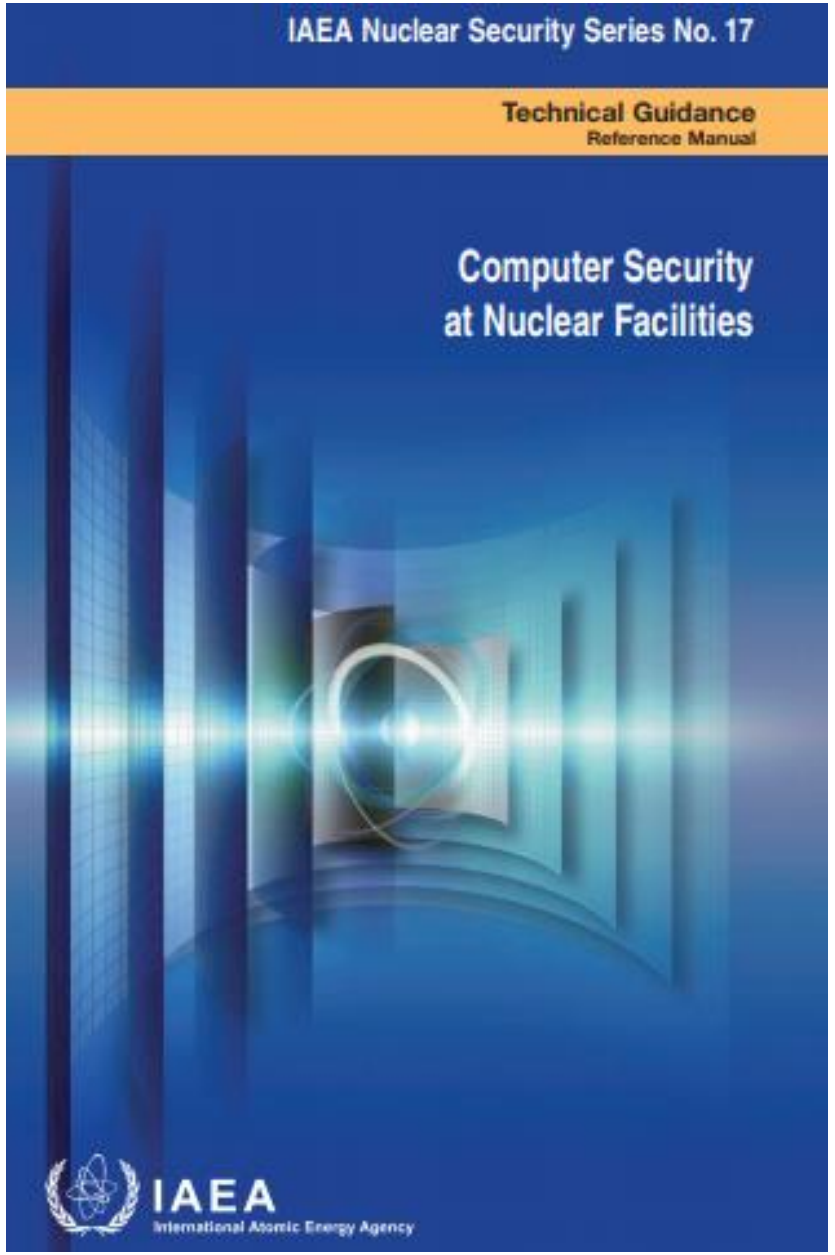
Existing Cyber-Nuclear Governance: Examples

<u>International Level</u>

- IAEA Nuclear Security Series No. 17 “Computer Security at Nuclear Facilities”
  - Provides non-binding guidance for the nuclear industry with a focus on best practices and lessons learned from nuclear and other critical infrastructure. Compliance is voluntary.
- Tallinn Manual on International Law Applicable to Cyber Warfare
  - Non-binding report written in association with the NATO Cooperative Cyber Defense Centre of Excellence that outlines legal responsibilities for cyber attacks.

<u>National Level</u>

- National regulations and law
- Design basis threat
- Corporate actions and requirements



AI Governance

International Level

- Currently does not exist.

National Level

- Many different documents, no cohesive strategy.
- U.S.
  - Preparing for the Future of Artificial Intelligence (2016)
  - National Artificial Intelligence and Development Strategic Plan (2016)
- China
  - New Generation AI Development Plan (2017)
  - Created two new institutions in 2017 – National Engineering Laboratory of Deep Learning Technology and AI Plan Promotion Office within the Ministry of Industry and Information Technology.
- Japan
  - Proposed 9 Principles for AI R&D at the 2016 G-7 Summit.
- South Korea
  - Robot Ethics Charter

PARTNERSHIP for GLOBAL SECURITY
LEADING THE WORLD TO A SAFER FUTURE

Considerations for Cyber and AI Governance

Some Concepts to be Considered from other Transnational Issues:

- Voluntary commitments vs. mandates
  - Mandates have been difficult to achieve and implement.
- Commercial innovation vs. government agreements/regulations
  - Government imperatives can be out of synch with market objectives, and the commercial sector is investing in and driving these technologies.
- Ad hoc approaches vs. weak Institutions
  - The reliance on the prerogatives of sovereign nations in international institution has limited their potential effectiveness; ad hoc approaches are more flexible but not deeply institutionalized.
- Incentivizing compliance vs. voluntary participation
  - In some cases, particularly nuclear, health, and climate requirements go unheeded because of lack of funds for implementation.

PARTNERSHIP for GLOBAL SECURITY
LEADING THE WORLD TO A SAFER FUTURE

Potential Trajectory of Cyber-AI Governance

- International cyber and AI governance may not result in the creation of a formalized institution, but rather a collaboration of various institutions, governments and the private sector. In order to achieve this model:
  - Multi-sector cooperation is essential between: governments of major cyber and AI players; governmental technical institutions and national laboratories; private sector and technical community; civil society; and existing international organizations.
  - Governments and the private sector will need to find a balance between their interests and objectives.
  - Existing institutions must be adaptable, willing to take on new arrangements, and manage new areas.
  - A system that incentivizes action will be needed.

PARTNERSHIP for GLOBAL SECURITY
LEADING THE WORLD TO A SAFER FUTURE

Developing Nuclear-Cyber-AI Governance

- Role of NE Asia Nuclear Security Institutions will be critical – South Korea, Japan, and China are all major players on cyber and AI technologies.
  - Nuclear Security Centers of Excellence – INSA, ISCN, SNSTC
  - KINAC
  - Others
- Proposals for activities:
  - Identifying technical needs and gaps and how they can be addressed.
  - Developing coordinated and integrated training on cyber and AI challenges and governance responses.
  - Instituting a regular forum (yearly) on nuclear-cyber-AI developments, challenges and responses.
  - Strengthening the role of IAEA in providing guidance and coordinating countries.
  - Collaborating with key institutions, industry organizations and NGOS in North America and European Union.