

Workshop Report

ISCN-CSIS Washington Workshop 2016 Nuclear Security Collaboration Between CoEs and Civil Society: Filling the Gaps

DIRECTOR AND SENIOR FELLOW

Sharon Squassoni

September 2, 2016



Introduction

On July 21, 2016, the Center for Strategic and International Studies (CSIS) Proliferation Prevention Program (PPP) and the Japanese Atomic Energy Agency (JAEA) Integrated Support Center for Nuclear Nonproliferation and Nuclear Security (ISCN) co-hosted a workshop on Center of Excellence (CoE) Collaboration with Civil Society, with a particular emphasis on the growing cyber threat to nuclear facilities. The workshop took place in Washington, D.C. at CSIS headquarters.

This meeting builds on previous CSIS-JAEA workshops. In 2015, participants explored potential areas of cooperation between Centers of Nuclear Security Excellence and civil society and industry globally and addressed ideas for sustaining the CoEs after the conclusion of the Nuclear Security Summits.

Mr. Kazunori Hirao of JAEA opened the workshop with a brief overview of the history of Japan's CoE and its collaboration with CSIS. He stressed the importance of international cooperation in sustaining the momentum of the Nuclear Security Summits and expressed pride at ISCN's accomplishments in infrastructure development and capacity building since its inception in 2010. U.S. Ambassador Bonnie Jenkins underscored the importance of sustaining the momentum of the summits, potentially through the Nuclear Security

Support Center (NSSC) network. She also noted the importance of the Contact Group created at the 2016 Summit in helping to sustain momentum. Ms. Sharon Squassoni of CSIS recognized two key areas of success since last year's CSIS-JAEA meeting on CoEs: improved cooperation regionally and bilaterally, through training initiatives; and improved coordination globally, primarily through the International Network for Nuclear Security Training and Support Centers (NSSC). She expressed hope that this year's workshop could identify further areas for cooperation.

Session I: Cyber security

Mr. Nima Ashkeboussi of the Nuclear Energy Institute provided the context for discussions on cyber threats and cyber security, beginning with an overview of the approach of the U.S. Nuclear Regulatory Commission (NRC) and U.S. nuclear industry generally in promoting cybersecurity of nuclear facilities. Mr. Ashkeboussi noted that the industry's involvement in cybersecurity predated the terrorist attacks of September 11, 2001, beginning in earnest with preparations for potential upheaval from the so-called Y2K phenomenon (the potential collapse of computer systems using only two-digit representation for years, thus failing to adapt to the turn of the century). The NRC issued cyber security regulations in 2009, with industry implementing key measures

of their program in 2012. Full implementation at all nuclear facilities will be achieved by 2017, with design-basis threats (DBTs) regularly updated to reflect the constantly evolving nature of cyber threats. Mr. Ashkeboussi identified portable media as a significant threat and noted several key challenges nuclear operators face, including information sharing across industries. While all cyber-attacks (even if unsuccessful) on nuclear facilities are reported to the NRC, the U.S. government also has important information about potential threats that needs to be disseminated. One participant argued that the government actually relies on reports of attacks from the industry, but conceded that the government could play a role in sharing information of those attacks with other nuclear operators or different industries.

Though all employees receive some degree of training (currently provided largely by contractors), information technology staff, engineers and operators, rather than security guards, are largely responsible for most of the daily implementation of cyber security measures and best practices. Mr. Ashkeboussi noted that from a financial standpoint of uninterrupted operations, nuclear energy facilities have incentives to ensure their sites are secure from cyberattacks, but expressed concern that the existing regulations are far broader than necessary—extending to items that are not required to prevent radiological sabotage or theft and diversion. The safety and control systems at U.S. nuclear energy facilities are not connected to the internet and the industry maintains that it is secure from a cyber-attack and, as a result of the enhancements made to plant operations,

the worst damage that could result from a cyber-attack is a safe shutdown of the reactor. One participant noted that while key systems may not be connected to the internet, the invulnerability of air-gapped systems is a myth, for systems often require connectedness to conduct temporary maintenance or install updates.

Mr. Ashkeboussi also presented an overview of enhancements in radiological source security since September 11, 2001, including differentiating between the regulations and rules issued by the NRC. He also described efforts to establish a near-real time database of the locations of all IAEA Category I and II sources in the United States, which is shared with the Federal Bureau of Investigation (FBI) and other intelligence agencies.

Ms. Naoko Noro of ISCN next explained that Japan strengthened the cyber security regulation in 2012 to incorporate the latest



*Figure 1 Computer Security in a Nuclear World on June 1, 2015.
Photo Credit: Dean Calma / IAEA*

IAEA recommendations on nuclear security. Ms. Noro identified the lack of trained personnel as the key challenge for cyber

security, noting that while there are experts in IT security, industry control systems for nuclear plants, or physical security, there are few individuals with knowledge of all three. Physical security personnel are often responsible for implementing cybersecurity measures in Japan. Ms. Noro pointed out that awareness of cybersecurity is not as pervasive in Japan as in the United States, but Japan recognized the importance of the issue and offered its first training course in 2014—a collaborative effort between the IAEA and the Japanese Center of Excellence, ISCN. One participant noted that the lack of expertise is a challenge shared by the United States and, as a result, the financial costs of training personnel and implementing cyber security measures are quite high.

Mr. Oleg Demidov of the PIR Center addressed the current nuclear cybersecurity regulatory structure in Russia and provided participants with an overview of past cyber incidents at nuclear facilities. Although cyber security requirements in Russia were initially motivated by the need to ensure confidentiality as a top priority (in competition with integrity and availability), this has gradually shifted in the last twenty-five years. The Russian government has issued several executive orders in the last five years that outline requirements for civilian nuclear installations, but executive orders are in some cases unenforceable without an associated federal law to provide the basis for implementation. The previous attempts to draft comprehensive legislation on information security of critical infrastructure, including the peaceful nuclear sector, failed due to diverging views and overlapping responsibilities.

Without a federal law to require implementation of CI cybersecurity measures, nuclear power plants in Russia lag behind in “cybersecurity by design,” in contrast to their physical protection measures. Mr. Demidov noted that a latest generation nuclear power plant can require more than 300 IT vendors to provide more than 10,000 sensors, which operate at 200,000 parameter variations per second. However, there is no complete list of vendors to ensure security, and Mr. Demidov raised the question of whether vendors should be required to provide source code of the critical field devices’ firmware to ensure the absence of covert programs or access points. One participant argued that this requirement would necessitate extremely burdensome and costly man-hours to comb through the code by hand, which would have to be repeated each time software updates are made.

Dr. Page Stoutland of the Nuclear Threat Initiative (NTI) noted positively that awareness of cybersecurity is growing, but that significant challenges remain in combatting the threat. Dr. Stoutland described current efforts to address cybersecurity at nuclear facilities as piecemeal and unable to keep up with the constantly evolving threats. He advocated for approaches that looked beyond technical measures, noting that technology can mitigate the threat but not eliminate it. According to NTI’s Nuclear Security Index, nearly half of the 47 countries surveyed with weapons-useable material or nuclear facilities at risk of sabotage had no national-level regulations in place to protect against cyber-attacks—Dr. Stoutland cautioned that the report did not attempt to measure the

effectiveness of the regulations where they do exist.

There are many barriers to international cooperation and information sharing, including a desire to keep countermeasures secret, and nuclear newcomers are particularly ill-equipped to combat cyber threats. Dr. Stoutland identified several potential areas for increased cooperation, including tabletop exercises and an international response team to provide support to mitigate the damage of an attack and assist recovery. Workshop participants discussed the possibility and desirability of creating a program similar to the U.S. Department of Energy's Nuclear Emergency Support Team (NEST) to respond to a cyber-attack on nuclear facilities.

Ms. Mizuki Hirai of ISCIN stated ISCIN has little experience engaging in public outreach activities in the nuclear security field, because the target participants of the ISCIN courses are generally working in the nuclear industry. Ms. Hirai also noted that, while the importance of public outreach in the field is unquestionable, it is still unclear who should take initiatives, what are the appropriate topics and what type of information should be shared with the public when doing outreach activities.

One participant noted that, for the general public, high-profile events like the Nuclear Security Summits can provide a false sense of confidence in the current security of nuclear materials and facilities. Another participant noted that the lack of discussion of cyber threats in particular can extend to the expert community, too—citing the example of a nuclear engineer for whom questions of cryptography are seemingly distant concerns. The IAEA hosted its first international conference on computer security in 2015, but greater engagement and collaboration across sectors involved in nuclear-related activities—including across different vendors—would be valuable. Greater communication will also help newly nuclear countries build capacity to respond to cyber threats, though one participant noted that even countries with long nuclear histories have significant room for improvement in developing cybersecurity regulations.

Session II: Building Public Confidence

The final portion of the workshop centered on questions of communicating risks to the public.

Participants discussed at length the role of civil society in communicating with the public and serving as a nuclear industry watchdog. While much information about cyber threats to nuclear facilities or possible countermeasures is classified, one



Figure 2 Conference on Computer Security in a Nuclear World on June 1, 2015.
Photo Credit: Dean Calma / IAEA

participant suggested that an organization like the Union of Concerned Scientists, which already serves as a watchdog with security clearance access to nuclear information, could provide an assessment of countries' ability to detect, defend against, and respond to attacks. Another participant noted the value of ensuring that there are well-informed experts on nuclear and cybersecurity issues, arguing that if a crisis does occur, the public will turn to the experts for guidance. Lastly, one participant noted the value of participation in workshops and training programs bringing together academics, policymakers, civil society members, industry officials, and emergency response personnel for cross-fertilization of approaches and best practices.