



Taking the Long View in a Time of Great Uncertainty

New Challenges for the Institute

Jack Jekowski

Industry News Editor and Chair of the Strategic Planning Committee

This year's 59th Annual Meeting, held at the Marriott Waterfront in Baltimore, was a nonstop, action-packed event that incorporated new formats, interactive panel sessions, and challenges presented to the Institute to ensure it stays on the leading edge of technology and policy. From the Opening Plenary to the close, attendees were provided a look into the future of nuclear materials management, and in the Closing Plenary, they were able to participate through a special interactive polling session to provide their own perspective of the future challenges that the world and the Institute will face.

The Second WINS Challenge

During the Opening Plenary¹ — in addition to two excellent speakers, Dr. Maria Betti and Dr. Brent Park — Will Tobey, the chair of the World Institute for Nuclear Security (WINS) provided a 10-year anniversary update of the activities of that international organization. Describing the INMM as the “father of WINS,” he recounted how Charles Curtis had challenged the Institute in 2005 in the Opening Plenary of the 46th Annual Meeting to establish a new organization to develop and share best practices in nuclear security management. Our own president, Corey Hinderstein, and other members of the Institute participated in a Strategic Planning Group that took that challenge and established WINS as an internationally recognized organization in September 2008 in Vienna. Ten years later, there are over 4,700 members in more than 128 countries, and over 1,000 participants worldwide, in the WINS

Academy, with 292 Certified Nuclear Security Professionals. WINS has hosted over 80 International Best Practices Workshops and produced 35 International Best Practices Guides. On this tenth anniversary, Will presented a new challenge to the Institute:

“By 2025, every person in this room, and every person worldwide who is employed professionally in the nuclear materials management, security, nuclear forensics, and safeguards fields will have the opportunity to take certified professional development courses to help demonstrate their professional competence.”

This new challenge, which WINS proposed to be supported by both them and INMM, is to the membership and their organizations to take the lead role. Fortunately, this is a strategic topic that has been discussed in the Executive Committee (EC) for the past two years, which culminated in a pilot professional development certification course offered to Annual Meeting attendees by Texas A&M University, entitled “Policy and Technical Fundamentals of International Nuclear Safeguards.”² Sixty-seven attendees took advantage of this comprehensive online course, which was capstoned by presentations during a special four-hour session of international experts Sunday morning prior to the start of the Annual Meeting. In producing, organizing, and following through on this course, Dr. Sunil Chirayath³ pioneered the concept that supported the

new WINS Challenge. Now it is up to us to develop the relationships with external organizations, including our National Laboratories in the United States and other institutions and organizations worldwide, to make this a reality.

The Cyber Challenge

Tuesday evening the newly formed Cyber/Physical Security Integration Committee met to discuss newly developed bylaws and an agenda for the coming year. This new committee was the result of strategic discussions by the EC during the past year as the Institute, like much of the rest of the world, has been faced with cyber challenges. The new committee has been established as a temporary resource for the technical divisions to integrate relevant cyber- and cyber-physical-security concepts and applications in pertinent areas of nuclear materials management. Dave Lambert, who was a guest columnist for us in 2016 when he was working in Kazakhstan,⁴ is the new chair of the committee, having returned to the United States as director of Gregg Protections Services, LLC. He has re-engaged with the Institute, having previously served as the chair of what is now the Nuclear Security and Physical Protection Technical Division, and he is now leading this new committee to ensure that cyber is integrated into all of the work of the Institute.

Since cyber issues impact all aspects of the Institute's mission, the EC believed it was important to establish this cross-cutting committee to work with all of the technical divisions to identify topics that impact



them, encourage papers and workshops, and continue to provide value-added information for our membership. The importance of the cyber environment is, of course, around us every day, from identify theft at the personal level to efforts influencing national elections, disrupting infrastructure, and stealing state secrets and industrial technologies.

Most recently in the United States, we have seen the following indicators of how influential this issue has become:

- Standup of the U.S. Cyber Command (USCYBERCOM) as the U.S. 10th Unified Combatant Command on May 4, 2018. Originally established as a subcommand under U.S. Strategic Command, CYBERCOM is now at the same level as other unified combatant commands and will be led by a four-star general. The new command will include 6,200 personnel organized into 133 teams, including active service members as well as members of the Reserve and National Guard.⁵
- A new office of Cybersecurity, Energy Security, and Emergency Response (CESER) has been established in the DOE.⁶ This new office will focus on energy infrastructure security, support the expanded national security responsibilities assigned to the Department, and report to the Under Secretary of Energy.
- On July 31, 2018, Homeland Security Secretary Kirstjen Nielsen announced the creation of a new center to share threat information with private companies at a Cybersecurity Summit held in New York City with several other high-ranking Administration officials and industry leaders, include Secretary of

Energy Rick Perry. The National Risk Management Center is expected to provide a central location for cybersecurity solutions nationwide.⁷

- As regards the new NSA Cyber Operations Center, the National Security Agency and Cyber Command marked the official opening of a new \$500 million building on May 4, one that is designed to integrate cyber operations across the U.S. government and foreign partners. The new Integrated Cyber Center and Joint Operations Center (ICC/JOC) is Cyber Command's first dedicated building, providing the advanced command and control capabilities and global integration capabilities needed to perform their missions.⁸
- Despite the complexities and resultant risks of the new cyber world, the DoD is moving toward cloud solutions for much of their data, including releasing a \$10 billion request for proposals for the Joint Enterprise Defense Infrastructure (JEDI), which could potentially house nuclear weapons design data.⁹

In the international community, we have the following recent developments:

- NATO: At the Brussels Summit in 2018, Allies agreed to set up a new Cyberspace Operations Center as part of NATO's strengthened Command Structure.¹⁰ Discussions are also underway to better define the level of cyberattack that would provoke a response under Article 5 of the NATO Charter, which is the alliance's principle of collective self-defense.¹¹
- European Union: The EU is planning to enhance its cyber-resilience by

setting up an EU-wide certification framework for information and communication technology (ICT) products, services, and processes.¹²

- Nuclear Threat Initiative: The Initiative has documented international cyberthreats in several reports, examining the vulnerabilities of nuclear material and facilities.¹³

As the world prepares for this new "battlefield," we will see this new committee engage with the technical divisions and open up new discussions, encourage papers, and facilitate panels for upcoming Annual Meetings.

The Challenges That Lie Ahead — Closing Plenary

An extraordinary Closing Plenary was held in Baltimore this year, moderated by then-President Corey Hinderstein (in her final year in that role), and designed to challenge the membership to think about the future of the Institute through a series of seven questions¹⁴ created by the EC as a component of our new Strategic Plan. Stimulated by an international panel of five experts,¹⁵ attendees were able to register their perspectives on remote polling devices, and results were documented to compare and contrast the perspectives of the five experts to the weighted perspectives of the attendees. Corey expertly coaxed feedback from the panel as well as from attendees to draw out the details of these perspectives. The results of this exercise will be used by the EC to help craft priorities for the Institute over the next couple of years, including a focus on future themes for the Annual Meeting.

This column is intended to serve as a forum to present and discuss current strategic issues impacting the Institute



of Nuclear Materials Management in the furtherance of its mission. The views expressed by the author are not necessarily endorsed by the Institute but are intended to stimulate and encourage JNMM readers to actively participate in strategic discussions. Please provide your thoughts and ideas to the Institute's leadership on these and other issues of importance. With your feedback, we hope to create an environment of open dialogue, addressing the critical uncertainties that lie ahead for the world, and to identify the possible paths to the future based on those uncertainties that can be influenced by the Institute. Jack Jekowski can be contacted at jjjekowski@aol.com.

Endnotes

1. The Opening Plenary session this year was streamed live and is archived on YouTube (www.youtube.com/watch?v=Nh2vSK4gyVs&feature=youtu.be). The presentation and challenge by Will Tobey can be seen beginning at 1:40:30 of the video.
2. See <https://nsspi.tamu.edu/nsspi-conducts-workshop-on-policy-and-technical-fundamentals-of-international-nuclear-safeguards>
3. Dr. Chirayath is an associate professor in the Nuclear Engineering Department, director at the Center for Nuclear Security Science & Policy Initiatives, and an honorary professor at Amity Institute of Nuclear Science & Technology.
4. See Jekowski, J. 2011. Taking the Long View in a Time of Great Uncertainty: A View from the International Community, *JNMM*, 44:4, 52–54.
5. See www.dodlive.mil/2018/05/03/cybercom-to-become-dods-10th-unified-combatant-command
6. Karen S. Evans was sworn in by U.S. Deputy Secretary of Energy Dan Brouillette as the Assistant Secretary for the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) on September 4, 2018. See www.energy.gov/ceser/ceser-leadership
7. See www.dhs.gov/sites/default/files/publications/national-risk-mgmt-fact-sheet-08282018-508.pdf and www.wired.com/story/dhs-national-risk-management-center
8. See www.fifthdomain.com/dod/cybercom/2018/05/07/cyber-command-nsa-open-new-500-million-operations-center
9. See www.nextgov.com/emerging-tech/2018/05/pentagon-wants-cloud-secure-enough-hold-nuke-secrets/148192
10. See www.nato.int/cps/en/natohq/topics_78170.htm
11. See www.nato.int/cps/en/natohq/topics_110496.htm
12. See www.consilium.europa.eu/en/press/press-releases/2018/06/08/eu-to-create-a-common-cybersecurity-certification-framework-and-beef-up-its-agency-council-agrees-its-position
13. See www.nti.org/media/documents/NTI_CyberThreats_FINAL.pdf and www.nti.org/analysis/reports/outpacing-cyber-threats-priorities-cybersecurity-nuclear-facilities. Also see <https://ntiindex.org/news-items/important-nuclear-security-progress-now-in-jeopardy-according-to-2018-nti-index>
14. Seven questions were provided to the panelists prior to the Closing Plenary, with several multiple choice answers, including “other.” After asking the attendees for their input, the panelists and the attendees were queried for more details. The questions posed were: (1) What is the current top global challenge/risk/threat with respect to nuclear proliferation? (2) What is the current top global challenge/risk/threat with respect to nuclear security? (3) Which risk set concerns you more? (4) What are the greatest cyber threats related to nuclear materials management? (5) What are the top 3 areas the INMM should focus on? (6) Which technology has the best chance to become a “game changer” (plus or minus), for the INMM? (7) Where should the INMM increase its attention?
15. Panelists included Dr. Jacques Baute, Director, Division of Information Management, Department of Safeguards, IAEA; Dr. Bassam Abdullah Ayed Khuwaileh, Assistant Professor, Nuclear Engineering Program, University of Sharja; Mitsuo Koizumi, Manager of Technology Development Promotion Office of Integrated Support Center for Nuclear Nonproliferation and Nuclear Security of the Japan Energy Atomic Agency; Sonia Fernández-Moreno, Planning and Evaluation Officer, Brazilian-Argentine Agency for Accounting and Control of Nuclear Materials; and Julie Oddou, Head of the Committee Technique Euratom, Atomic Energy Commission (CEAR).