Developing a multi-year nuclear-cyber capability development training and education program

Zong Bo [1], Xiaojun Liu [1], Charles Nickerson [2], and Chris Spirito [2]

[1] State Nuclear Security Technology Center of China, Beijing, China
[2] Idaho National Laboratory, 2525 Freemont Ave., Idaho Falls, Idaho, USA

Abstract

The cyber domain has evolved over the past thirty years from one that was primarily concerned with the protection of data confidentiality, integrity, and availability, to one that includes an integrated set of defensive technologies and processes in order to respond to the ever-advancing threats posed by skilled cyber actors. As the cyber threat actors have evolved their capabilities, it has required that defenders not only deploy defensive cyber capabilities and skilled cyber defense staff to handle these tools and data, but also extend their training and education programs to include all staff such that the entire organization is considered as part of the cyber defense team, identifying and reporting observations that may indicate that a cyber-attack has or is taking place.

The nuclear domain for this same thirty years has included programs to address the protection and nonproliferation of nuclear materials through programs for physical security protection, insider threat mitigation, nuclear material control and accounting, transportation security, protection from sabotage, and incident response. It is only in the past ten years that cyber-security has become a capability of concern, not only as applied to these existing security domains, but also by itself as the attack surface within a nuclear facility is large and includes interaction with a diverse multifunctional staff. To address these security concerns countries such as China and the United States have established nuclear security centers of excellence in support of developing capabilities that contribute to mitigating the overall risk of handling and using nuclear materials.

Over the past three years the US and China have been working together at the State Nuclear Security Technology Center (SNSTC) in Beijing, China to implement a multi-year nuclear-cyber capability development training and education program. This program was built referencing US NIST Special Publication 800-50 on building an Information Technology Security Awareness and Training Program that includes a basic curriculum allowing students to progress from awareness programs to training courses to specialized domain education, with all course materials derived from existing risk and threat assessments. These courses are being implemented at the Center of Excellence in Beijing that is a multi-building site modeled with common nuclear facility capabilities including physical security zones and associated protection technologies, a functional Central and Secondary Alarm Stations (CAS/SAS), a material processing facility, and a material storage vault. This infrastructure allows for all courses from awareness through advanced to be offered with a hands-on component.

This paper presents the co-developed capability development training program including a history of the courses conducted that informed the creation of the structural levels and how this information was mapped to China's existing operational training programs for completeness. Program course levels include awareness, basic training, intermediate-to-advanced training on specific topics, and educational initiatives in conjunction with national universities. Our paper also includes information on how cultural issues were handled in the development and delivering of courses and how these courses have benefited the overall US-China confidence building process within the nuclear-cyber community.

Keywords: Nuclear-Cyber, Training and Education, Multicultural Exchange, United States, China

1.0 Introduction

In most circumstances, the ***Abstract*** for a conference paper should be written after the paper itself is complete so that outcomes from the research can be represented alongside the methodology used to arrive at that point. And like so many others who are writing Introductions we have looked back upon our Abstract to better understand what the heck we were thinking when we wrote the eloquence you surely just read, now having arrived at the ***Introduction*** with bated breath. Before we begin with the proverbial *meat* of the paper, we (the authors) should provide for you a few definitions for terms used in our title as our work may not be obvious for those outside of our community of nuclear-cyber experts.

What is Nuclear-Cyber?

The narrowest way to view *Nuclear-Cyber* is to think about all non-weapon related uses for nuclear material and how that material is sourced, transported, used, and stored with its byproducts for eternity. Take each of these processes and draw a picture of the machines used to accomplish these activities with the nuclear material. Finally perform an assessment of each of these machines, everything from drills and trucks to centrifuges and process controllers, and how the related operational data is protected to ensure ***confidentiality*** (only those who should see the data, see the data), ***integrity*** (the data arrives at its destination without error or tampering), and ***availability*** (the data is ready for use when needed). This is at the most basic level what we mean by ***Nuclear-Cyber***, the protection of core data processing functions of non-weapon related nuclear systems.

What is a Nuclear-Cyber Capability?

Following from our definition of *Nuclear-Cyber* we can then define a *Nuclear-Cyber Capability* as any process and associated procedures (actions) that allow us to ensure the confidentiality, integrity, and availability of non-weapon related nuclear systems. Simple right? Except this is the point that is a bit like watching two nuclei collide and trying to keep track of the subsequent chaos that is produced as while we can easily understand at a basic level what a Nuclear-Cyber capability is, the number of functionally associated sub-domains and their dependencies can feel entirely overwhelming. Specific Nuclear-Cyber capabilities would include being able to perform a risk assessment of a target system and choosing appropriate risk handling actions such as remediation and mitigation. Other capabilities include more targeted technical tasks such as the analysis of data on mobile media for malware and establishing processes for incident response should an abnormal event occur and need to be investigated. One goal of the joint team from the United States and China is to establish a training and education program that would allow the personnel working at Nuclear Power Plants (NPPs) and Fuel Enrichment facilities to acquire the knowledge necessary to ensure the safe handling of nuclear materials as related to the risks posed by using information processing systems that are known to be potential targets for cyber-attacks.

What is the difference between Training and Education?

This is an essential concept to understand as the program we have developed includes both acquisition of skills and integration of education to address long-term projected staffing needs. We define ***Training*** as focused on *Knowledge, Skills,* and *Attitudes (KSAs)* where *Knowledge* is defined as a set of information necessary to complete a task; *Skills* are actions that need to be performed where proficiency can be measured; and *Attitudes* is the mentality necessary to use the knowledge and skills operationally. We define ***Education*** as the process of investing in a specific area over an arbitrarily longer period of time that allows the student to learn the underlying theory and mechanisms of a subject, typically through lectures, laboratories, and guided mentorship.

2.0 History of courses conducted at the SNSTC Center of Excellence (CoE)

In 2016 the Department of Energy (DoE) National Nuclear Security Administration (NNSA) created an Introduction to Nuclear-Cyber training course. The purpose of this training was to introduce attendees to the concepts of digital systems, cyber security, cyber threat actors and their capabilities, and incident response. In the first year this course was offered attendees from Nuclear Power Plants and Research Reactors, Nuclear Regulators, and other associated facilities, spent five full days with two US National Laboratory Instructors receiving lectures (80%) and participating in group exercises (20%) to become familiar with the developed content. In the Fall of 2016 this course was delivered for the first time at SNSTC CoE, marking the developmental starting point for our multi-year nuclear-cyber capability development training and education program.

Information Gathering and Course Customization

As would be expected, with each of our initial engagements we were able to learn more about the nuclear infrastructure in each country and assess what options we have available to us for future trainings. In some countries we would meet in conference centers or even hotels but the SNSTC is a special facility having been jointly built by the United States and China and containing a sizable mock-up of physical security zones and associated protection technologies, a functional Central and Secondary Alarm Station (CAS/SAS), a material processing facility, and a material storage vault. Additionally, the site had separate rooms for specialized training including a physical security technology laboratory which we integrated into our course curriculum in 2019.

Managing Cyber Risk (June 2018)

Based upon the lessons learned from teaching the Introduction to Nuclear-Cyber course a second course was developed by NNSA in 2017 called Managing Cyber Risk (MCR). The MCR course was created to span the course of 5 days and attempted to shift the lecture / group exercise ratio towards 50/50 including new hands-on modules such as methods to understanding and defeating motion detection systems. In June of 2018 we conducted a modified version of this MCR course in Beijing that was extended to 8 days over the course of two weeks. The preparation for this course took place in 2017 and early 2018 through a series of technical exchanges that allowed us to incorporate the environmental lessons learned from the first course with information about the current state of cyber-security implementations within the Chinese nuclear infrastructure and the content and structure of existing training and education programs.

Managing Cyber Risk (July 2019)

Just over one year later we conducted a new version of the MCR course with some well received structural changes. This version of the course was conducted over 5 full days and the ratio of lecture to group exercise improved to 30/70. We introduced into this version of the course a scenario that carried the students between modules throughout the week and incorporated both the physical plant infrastructure and the physical security systems testbed into the course. The course modules included performing a risk analysis of the facility, identifying critical digital assets, understanding threat actor capability, interrogating hardware and software for vulnerabilities, and engaging the incident response process.

Nuclear-Cyber Awareness (December 2019)

As part of the training program we have jointly developed, we will be conducting a new course in December 2019 on Nuclear-Cyber Awareness. This will be our first course offered to a class of students focused on concept awareness rather than in-depth technical KSA acquisition.

3.0 Multi-level, multi-year, training and education program

The goal of all training programs is to transfer the latest knowledge, skills, and attitudes to the students on a schedule that ensures that perishable skills are kept current and the latest evidence-based concepts are delivered to relevant personnel in a timely manner. During our technical exchanges in 2017 and 2018 we created a multi-level, multi-year, training and education program that both meets these goals as well and aligns with the goals of the Training and Education Directorate within the Chinese Atomic Energy Authority (CAEA).

Constraints and Existing Training Programs

Through the exchange of experts from China and the United States,One of the challenges faced by CAEA which is not uncommon throughout the global nuclear community is a lack of regulatory guidance for inclusion of cyber security controls within facilities that handle nuclear material. There is ample guidance available for Physical Protection Systems, Transportation, NMAC, and the usual family of nuclear support systems and activities but only a few nations at this point have guidance documented and even fewer have implemented their guidance throughout their fleet. This is an important point since any training and education programs will be based upon the regulatory requirements which in the case of cybersecurity generally call for a Cybersecurity Plan to be created that encompasses the Risk Management and Incident Response processes. Since China does not currently have these regulatory plans in place one of the constraints that we had to address was to develop this training program based upon US best practices with care to fit them to the environment where they are going to be deployed and within the existing education and training programs.

The existing training programs within China are conducted on site at the Nuclear Power Plants and Research Reactors and at the SNSTC where the use of the mock facility can be incorporated into the courses offered there. While the short-term goals are to implement a cybersecurity training program our mid-term goals include integrating cyber-security concepts into China's existing training programs such that there are multiple pathways for personnel to learn the cyber concepts and techniques necessary to perform their jobs and address the ever-changing and evolving threat.

Multi-level course offerings

While it may seem intuitive to structure educational initiatives in this way, care should be taken that there is ample functional separation between levels and that each level is able to accommodate the target knowledge and skills that the trainings will deliver for identified audiences. Figure 1 shows the approach used by NIST 800-50, a standards document on *Building An Information Technology Security Awareness and Training Program.* The multiple levels of planned courses include Awareness Activities and Workshops, Security Basic Training, Cyber Security for Specific Functions and Roles, and formal Education and the relationship between levels as viewed from a knowledge dependency point of view. Proposed target audiences for courses offered at each level are included. This provides for our curriculum development team the high-level insight necessary for both crafting the course inter-dependencies as well as curate content that can be delivered at the appropriate technical level of detail.

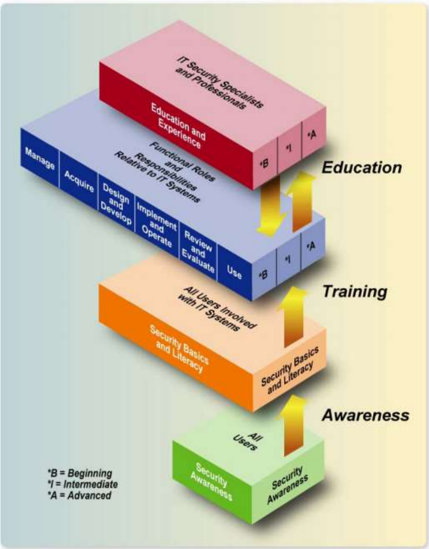

Figure 1 - Multi-level course offerings

Using the NIST 800-50 approach we proposed and agreed to the following Training Definitions as we move forward with implementation:

Awareness Activities/Workshops (Green)
- Designed to change behavior and reinforce good security practices across multiple disciplines
- Focus is on recognizing risks and personnel role in reducing cyber risks

Security Basic Training (Orange)
- Identify needed security skills and competencies
- Designed for personnel that interact with Critical Digital Assets within their environment
- Identify resources to develop requisite skills and competencies

Cyber Security for Specific Functions/Roles (Blue)
- Develop requisite skills and competencies for a specific job task or functional role.

Education (Red)
- Partnership with high learning institution (Tsinghua Univ)
- Outside scope of US/China Cyber collaboration

Multi-year course mappings

Once we had the levels defined, we were able to create an initial curriculum with educational pathways for students. Figure 2 depicts the courses and identifies the pathways that students are able to engage for progressing in their nuclear-cyber education. We have also mapped each of the courses to core cyber-defensive activities including: Identify; Detect, Protect, Respond, and Recover.

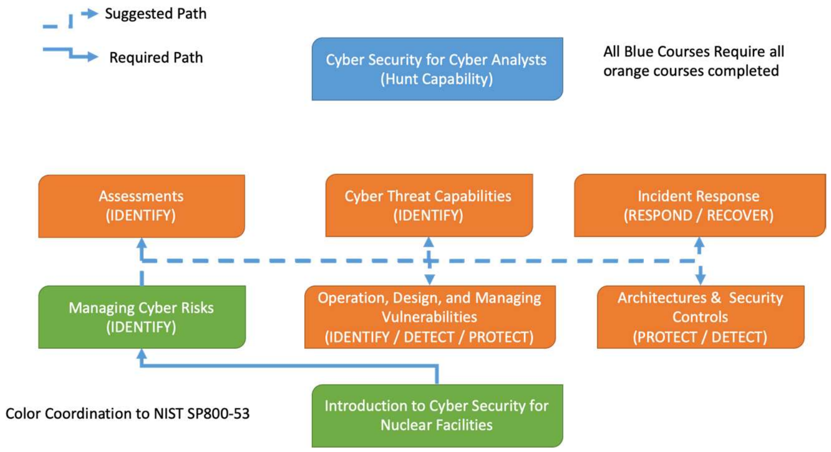
Suggested Path
Required Path
Cyber Security for Cyber Analysts (Hunt Capability)
All Blue Courses Require all orange courses completed
Assessments (IDENTIFY)
Cyber Threat Capabilities (IDENTIFY)
Incident Response (RESPOND / RECOVER)
Managing Cyber Risks (IDENTIFY)
Operation, Design, and Managing Vulnerabilities (IDENTIFY / DETECT / PROTECT)
Architectures & Security Controls (PROTECT / DETECT)
Color Coordination to NIST SP800-53
Introduction to Cyber Security for Nuclear Facilities

Figure 2 - Cyber-security Educational Pathways

The two courses in green are ones which have already been developed and delivered at the SNSTC. Generally, all students will start at the *Introduction to Cyber Security for Nuclear Facilities* course and then take the *Managing Cyber Risks* course. The five courses in orange exist at the intermediate training level and are pre-requisites for the blue courses which are targeted to functional roles and associated job responsibilities. We are currently working together to schedule the curriculum development and delivery timetable that will offer these courses at SNSTC and Chinese sites over the next five years. The long-term goal is to identify which skills will be needed in the future such that University programs can incorporate these courses into their curriculum.

4.0 University and International Agency Cooperation and Collaboration

Engaging Universities with SNSTC for Cyber-security training and education is the path to offering education-centered courses that can be included in our multi-level, multi-year cyber training and education curriculum, allowing personnel to gain a deeper understanding of the subject matter at hand. To understand this, consider Bloom's Skills in Cognitive Domains. Bloom defines Training as focused on: ***Application*** *(to apply concepts in new situations);* ***Comprehension*** *(understanding instructions and problems); and* ***Knowledge*** *(recalling data and information)*. Bloom defines Education as focused on: ***Evaluation*** *(making judgements);* ***Synthesis*** *(building structures from diverse elements); and* ***Analysis*** *(separating concepts into components)*. It makes sense why we are first focused on Training as Application, Comprehension, and Knowledge are essential to addressing cyber-threats that already exist in the target environment. Partnering with Universities allows the educational pathways to link into the overall plan and allows for the inclusion of long-term personnel planning.

As cyber mission sets grow over time, the cyber work force will need to adapt with the changing ambition and requirements. This will require an approach to recruitment that is capable of filling existing roles with competent personnel as well as identifying how many junior staff members will be required to meet the work force needs into the future (5-10 years). Using an existing and projected skills matrix personnel attributes can be identified that should be used for recruitment. These are the skills that should be targeted within University courses and associated curriculums as the goal is to graduate students who are ready to join the Nuclear-Cyber workforce.

Although it is not specifically addressed in our current plan there is also an immediate need for cyber-security managers within the Nuclear Regulatory Agency and reactor sites. These managers will need to lead, manage, and oversee cyber defense and cyber operations. These individuals do not necessarily need specific training in engineering or programming, but they must have a deep understanding of the cyber context in which they operate, compounded with an appreciation of ethics, strategic studies, political theory, institutional theory, international law, international relations, and additional sciences.[1]

[1] Spidalieri, Francesca. Joint Professional Military Education Institutions in an Age of Cyber Threats. 2013.

With a long-term goal of establishing a nuclear-cyber training and education ecosystem it makes sense to engage Chinese Universities, especially those that have programs in Nuclear Engineering, Computer Science, and Computer Security. Tsinghua University in Beijing has both an *Institute of Nuclear and New Energy Technology*[2] and a *Department of Computer Science and Technology*.[3] Through this partnership educational goals can be achieved, and advanced training can be linked to these courses through establishing apprenticeships for enrolled students.

Alignment with the IAEA Coordinated Research Project (CRP) J02008

While this is not formally represented in our plan, opportunities to collaborate with international organizations such as the International Atomic Energy Agency (IAEA) should be captured. For example, the IAEA CRP on Enhancing Computer Security Incident Response at Nuclear Facilities both included participation from Tsinghua University and produced a Nuclear Power Plant simulator specifically designed for as a cyber test-range. These capabilities should be considered for transfer.

5.0 Cultural Issues, Scallion Pancakes, and Confidence Building

We are pretty sure that more than a few eyes raise when seeing not only a paper jointly written by cyber-security experts from China and the United States but also to find out that we have been working together crafting a nuclear-cyber training and education program. We have arrived at this point through the usual dedication and hard work but also by recognizing that there were cultural issues that needed to be addressed early in our relationship. Spirito (me) describes this in his 2012 paper on trust relationships in a section titled *Information Value Perception and Collaborative Risk Management*:

> When we look further into how entities view of particular piece of data or situation, we find this topic explored by "ethnomethodologists", who use the phrase "sense-making" to refer to observable behaviors in which individuals orient toward the same aspect of the world and demonstrate to each other – through detailed enactment of practices – that they share that orientation. "Mutual orientation toward an object" includes:
>
> - Perception (we're looking at the same thing),
> - Interpretation or instructed perception (we're looking at the same aspects of, or applying the same framework on, that thing), and
> - Conventions or instructed actions (we display similar behaviors with respect to use of that thing; the modifier "instructed" refers to the fact that we learn those behaviors from one another, primarily by example)."[4]
>
> This first step in the analysis of an information sharing relationship is critical, especially when two or more countries and cultures are involved. There must be an agreement from all parties that the shared perception of the objects in the repository exists. The second step is to ensure that all parties agree upon the analyzed characteristics of the framework. Lastly, there needs to be an ability to include the behavioral components of information sharing so that acceptable boundaries are placed around. Standards ensure entities agree on the information to share and can exchange it.

These concepts were central to our success over the past three years as we continually worked with our interpreters to ensure that as we raised and parsed concepts to support the outcomes and deliverables we were producing, that we were aligned in perception of object, perception of framework and point of view, and agreement on conventions and instructed actions. Additional cultural aspects were also included that included: philosophy, motivation, ambition and commitments to transparency.

[2] Institute of Nuclear and New Energy Technology. https://www.tsinghua.edu.cn/publish/ineten/index.html

[3] Department of Computer Science and Technology. https://www.tsinghua.edu.cn/publish/csen/index.html

[4] Bodeau, D., Powers, E., Brooks, J. Making Sense Together: Applying Ethnomethodology to Enhance Advanced Systems Engineering in the Information sharing Domain

Scallion Pancake Diplomacy and Confidence Building

While this is not central to our work on this training and education program, there came a point in 2018 where the Chinese team requested an open-source document on a relevant aspect of cyber-security capability development. The US team was able to successfully negotiate a tray of scallion pancakes each visit in exchange for the document. While this event may seem like just a nice story, it is these types of interactions that help solidify the mutual trust developed between two parties and thus contribute towards confidence in both their relationship and their ability to engage on equal footing.

6.0 Conclusion

Retrospectively, our progress seems significant given the constrained environment that we are operating within but we hope that our past successes will continue to grow, beyond just what we are accomplishing in China, but also to include the creation of best practices that can be shared with other nations currently developing nuclear-cyber capability training and education programs. In between courses during our technical exchanges we also raise issues that should be considered at some point in the future. These issues include:

Should China's Atomic Energy Agency create a National Cybersecurity Professional Body?
Establishing any professional body takes time to both engage all of the relevant stakeholders and establish and execute a plan for implementation. The choices that CAEA, SNSTC, and Tsinghua University make now regarding their curriculums may be impacted by this type of decision so even if this is perceived to be a 5-year or further into the future goal, the topic should be raised for discussion in the near future.

Should the US and China Develop and Maintain a Professional Common Body of Knowledge (CBK)?
The field of cyber-security has been working off of a Common Body of Knowledge generally tied to the Certified Information Systems Security Professional (CISSP) certification. The CBK areas are well known in the cyber-security field and include areas such as *Security and Risk Management; Asset Security; Security Architecture and Engineering; and Security Operations*. Nuclear-cyber includes areas that are not a part of the CISSP CBK such as *Control Systems (PLCs)* and there are operational issues that are only found in industrial complexes where traditional mitigation and remediation solutions will not be possible.

How do we codify Establishing and Maintaining Required Levels of Training and Education?
The last topic is more of a policy and regulatory issue as any rules or concepts that will be applied to nuclear operational environments will need to be agreed to by, at the very least, the national regulatory body. The question that should be addressed at some point is how to accomplish this when the target is constantly moving. What we mean by that is that any planning that takes place today, assuming it will not be implemented for one-year, will be outdated by the time of implementation. Addressing this cycle will be critical to codifying any required levels of training and education.

Thank you for your time and attention.

"Some love is just a lie of the heart
The cold remains of what began with a passionate start
And they may not want it to end
But it will it's just a question of when
I've lived long enough to have learned
The closer you get to the fire the more you get burned
But that won't happen to us
Cause it's always been a matter of trust"

- Billy Joel, The Bridge, 1986