INL/CON-15-35137
PREPRINT

Understanding the Value of a Computer Emergency Response Capability for Nuclear Security

The International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange

Julio Rodriguez
Peter D. Gasper

June 2015

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

Abstract. The international nuclear community has a great understanding of the physical security needs relating to the prevention, detection, and response of malicious acts associated with nuclear facilities and radioactive material. International Atomic Energy Agency Nuclear Security Recommendations (INFCIRC_225_Rev 5) outlines specific guidelines and recommendations for implementing and maintaining an organization's nuclear security posture. An important element for inclusion into supporting Revision 5 is the establishment of a "Cyber Emergency Response Team" focused on the international communities cybersecurity needs to maintain a comprehensive nuclear security posture.

Cybersecurity and the importance of nuclear cybersecurity require that there be a specific focus on developing an International Nuclear Cyber Emergency Response Team. States establishing contingency plans should have an understanding of the cyber threat landscape and the potential impacts to systems in place to protect and mitigate malicious activities. This paper will outline the necessary components, discuss the relationships needed within the international community, and outline a process by which the International Nuclear Cyber Emergency Response Team identifies, collects, processes, and reports critical information in order to establish situational awareness and support decision-making.

Key Words: nuclear, cyber security, instrumentation and control, CERT.

CONTENTS

1. INTRODUCTION

The International Atomic Energy Agency (IAEA) Board of Governors approved the first concerted nuclear security plan in March 2002. The board approved the current *Nuclear Security Plan 2014–2017* (GOV/2013/37) in August 2013. This plan builds on general conference resolutions, the ministerial declaration and, where appropriate, the conclusions and recommendations from the conference. In addition, it consolidates activities set out in the *Nuclear Security Plan 2010–2013*, taking into account new and modified priorities of Member States. Among the desired outcomes listed in Section E.1 "Needs Assessment, Information and Cybersecurity" of the *Nuclear Security Plan 2014–2017* was: "Improved cybersecurity capabilities at the State and facility level to support the prevention and detection of, and response to, information security incidents that have the potential to either directly or indirectly adversely affect nuclear safety and nuclear security." [1]

This direction established a path forward for all member states and organizations to improve the cybersecurity posture. The following sections highlight key topics relating to recommendations, technical guidance, and implementation of actions designed to support the development of an International Nuclear Cyber Emergency Response Team (NS-CERT) to address the unique needs of all organizations identified in Nuclear Security Plan 2014–2017.

1.1. REQUIREMENTS FOR AND IMPLEMENTATION OF IMPROVED CYBERSECURITY

Specific statements of policy and research leading to the determination of need for "Improved cybersecurity capabilities" are documented in the following IAEA Nuclear Security Series (NSS) publications:

- NSS-13, *Nuclear Security Recommendations of Physical Protection of Nuclear Material and Nuclear Facilities* (INFCIRC/225/Revision 5), 2011 [2]
- NSS-17, *Computer Security at Nuclear Facilities*, 2011 [3]
- NSS-19, *Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme*, 2013 [4].

IAEA has developed these documents based on standards and practices by member states with the intention of providing overarching cybersecurity requirements (recommendations, technical guidance, and implementing guide). The key question becomes how will organizations use the information to develop and implement cybersecurity programs within their facilities? There is also the question of how they will ensure protection of nuclear materials and facilities based on their country's regulatory requirements and policies.

1.1.1. NSS-13 and Cybersecurity Requirements for Physical Protection of Nuclear Materials

Leveraging the recommendations provided in NSS-13, general cybersecurity requirements are based on two physical categories of threat: (1) unauthorized removal of nuclear material and (2) sabotage at nuclear facilities. Though somewhat nonspecific, NSS-13 does clearly identify "cyber-attack" as a potential threat to physical security. The requirements to protect nuclear materials and nuclear facilities from the physical threat posed by "cyber-attack" are described as:

- Unauthorized removal of nuclear material in uses and storage as set forth in Section 4.10 "Computer based systems used for physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise (e.g., cyber-attack, manipulation, or falsification) consistent with the threat assessment or design basis threat."
- Sabotage at nuclear facilities as set forth in Section 5.19 "Computer based systems used for physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise (e.g., cyber-attack, manipulation, or falsification) consistent with the threat assessment or design basis threat."

1.1.2. NSS-17 and Cybersecurity Requirements for Computers at Nuclear Facilities

The primary aim of NSS-17 "is to create awareness of the importance of incorporating computer security as a fundamental part of the overall security plan for nuclear facilities." The publication also provides technical guidance specific to nuclear facilities on implementing a computer security program and provides advice on evaluating existing program, assessing critical digital assets, and identifying appropriate risk reduction measures.[1]

Section 7 of NSS-17, "Special Considerations for Nuclear Facilities," provides extremely important insights on cybersecurity in the special context of systems-of-systems. It offers useful background discussion on weaknesses inherent in instrumentation and control (I&C) systems design. This section alerts nuclear community security professionals to a special set of cybersecurity challenges that are present in typical nuclear facilities.

1.1.3. NSS-19 and Implementation of a Cybersecurity Infrastructure

NSS-19 is the implementing guide designed to assist states in understanding and addressing the key actions to establish an effective national nuclear security infrastructure for a nuclear power program (NPP). It is intended to be used in conjunction with the Nuclear Security Fundamentals and various recommendations, as well as other IAEA NSS publications, as appropriate. Although cybersecurity (information security) is only specified once in this document, it is understood that the establishment of cybersecurity is an important component of the actions necessary to implement a coherent and integrated nuclear security infrastructure for an NPP.

2. IDAHO NATIONAL LABORATORY SUPPORT TO NUCLEAR CYBERSECURITY

The IAEA works for the safe, secure, and peaceful uses of nuclear science and technology. Recognizing that Idaho National Laboratory (INL) is a leader in the critical emerging area of nuclear cybersecurity, the U.S. and IAEA have engaged in numerous collaborations with INL in addressing cybersecurity.

---

[1] For additional information on critical digital assets, see the U.S. Nuclear Regulatory Commission's January 2010, Regulatory Guide, Office of Nuclear Regulatory Research, Regulatory Guide 5.71 Cyber Security Programs for Nuclear Facilities. http://pbadupws.nrc.gov/docs/ML0903/ML090340159.pdf and NEI 08-09 Revision 6, Cyber Security Plan for Nuclear Power Reactors, http://pbadupws.nrc.gov/docs/ML1011/ML101180437.pdf

Supported by U.S. government sponsors and private and international companies, INL has worked closely with the international community in developing and delivering training customized to the needs of various member states. For example, in 2013, INL provided international training for a Romanian National Training Course developed by the IAEA for nation states requesting computer security information for nuclear facilities. The INL also conducted the first-of-a-kind nuclear facility industrial control training for IAEA, providing I&C subject matter expertise in cybersecurity for a nuclear facility. INL has also hosted regional training courses for state inspectors conducting cyber security assessments at nuclear facilities as well as participated in numerous cybersecurity assessments.

2.1. NUCLEAR CYBER THREAT – INCREASED INDUSTRIAL CONTROL SYSTEMS PRESENCE AND EXPOSURE

In 2008, INL estimated there would be an increased threat to critical infrastructure industrial control systems (ICS) during 2010–2015 due to the growing "presence and exposure" of those systems [5]. By inference, this forecast also applies to the domain of nuclear security administered by the IAEA because of increasing reliance on I&C at nuclear facilities.

2.1.1. Continuing and Emerging Trends in Cybersecurity

The increased threat projection was based on analysis of five significant, emerging trends:

Trend 1—Proliferation of ICS: Nearly all sectors of critical infrastructure are moving towards advanced automation using ICS.

Trend 2—Increased Digital and Internet Protocol Base: ICS networks are digital and internet protocol based. Control systems that rely solely on "plain old telephone systems" also have digital components. In addition, on top of the general digital/internet protocol base runs a profusion of different control systems protocols.

Trend 3—Expanded Use of Wireless Communications: International Data Corporation estimates there will be 200 billion connected devices by 2020 and Cisco estimates the market size at $14.4 trillion (£9.6 billion[2]). This striking growth highlights concerns over the security of many modes of wireless communications paths developed for ICS.

Trend 4—Impediments to Security Measure Implementation: In addition to ICS growth and proliferation trends, is the trend to improve ICS security. While many successful initiatives to introduce security systems and mitigate known vulnerabilities occur, other security programs are impeded by economic and organizational factors.

Trend 5—Advent of Systems-of-Systems and Internet of Things: As a natural consequence of evolution within Trends 1, 2, and 3, a tendency towards convergence among their related technologies has appeared. ICS are becoming less identifiable as independent elements of emerging

[2] Mark Morley's article "Internet of Things brings a sense of purpose to cloud, mobile and Big Data," accessed at http://betanews.com/2015/03/30/internet-of-things-brings-a-sense-of-purpose-to-cloud-mobile-and-big-data/.

systems within given facilities. The systems are absorbed into an “internet of things” connecting multiple facilities and functions.

Thus, these five identified trends signal the need for greater attention to the problem of reduction of vulnerability potential by means of decreasing exposure of ICS. Unfortunately, Trends 4 and 5 add to the difficulty and cost associated with any effort to decrease ICS exposure.

2.2. IAEA CYBER SECURITY PROGRAM – RECOGNITION OF THE THREAT

The media constantly informs us that the predicted vulnerabilities and threats have become realities. For example, the adjacent chart illustrates the number of U.S. Department of Homeland Security (DHS) ICS Cyber Emergency Response Team (ICS-CERT) responses to cybersecurity threats across the critical infrastructure sectors. During fiscal year 2014, 6.2% (~15) of ICS-CERT responses were to events at or related to nuclear facilities (see FIG. 1) [6].

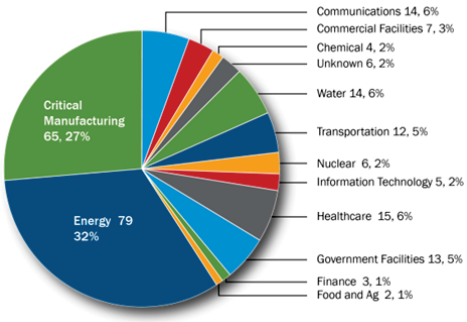

FIG. 1. ICS-CERT 2014 year in review.

A briefing presented by the IAEA Nuclear Security Information Officer, in May 2013, provides an excellent overview of IAEA information and computer security with emphasis on threat [7]. This discussion demonstrates that there are an increasing number of nuclear-related targets for cyber-attack. Among the most significant of the new targets is technology used in nuclear I&C.

The threat briefing compares the evolution of information technology security and control system and then provides examples of network attacks on ICS networks. The presentation highlights the cyber-physical aspect of ICS vulnerabilities as shown in the "Aurora" generator test conducted by DHS at INL in March 2007. A very important lesson learned from this test was: "Physical equipment can be damaged solely by cyber means."

2.3. THE NATURE OF THREAT

"Threat" is commonly, although not consistently, defined as:

Threat = Capability + Intent + Opportunity.

FIG. 2. Threat diagram.

From the analytic perspective, the definition assumes the existence of a threat "source," which is an actor or agent posing the threat. For many reasons, the vulnerability assessment process is developing at a faster pace than the threat assessment process. While vulnerability assessment aids in estimating the capability factor in the threat equation, satisfactory assessment of intent and opportunity is more difficult. The primary focus of cyber threats to NPP is on I&C. These systems consist of a set of hardware and software acting in concert that gathers information and then performs physical functions based on established parameters and/or information it received [5].

FIG. 2 depicts the commonly accepted components of threat including the concept of opportunity and hostility. It also shows how the intersection between the various elements of threat can be used to depict various threat states posed by threat actors:

- **Impending threat** is the combination of capability and hostile intent. Without the opportunity to act, the threat remains in the impending stage and is dormant.

- **Potential threat** is the combination of capability and opportunity. Without hostile intent, this threat remains in the potential stage. This is the primary vector of the insider threat. They have opportunity and capability but generally no hostile intent until something causes them to change their motivations.

- **Insubstantial threat** is the combination of hostile intent and opportunity. Without the capability, many attempts to act will fail or turn out to be insubstantial.

3. CERTS – HISTORY AND PERSPECTIVES

CERTs represent cyber domain expert groups that handle computer security incidents. Alternative names for such groups include computer emergency readiness team, computer emergency response team, cyber emergency response team, and computer security incident response team. The name CERT is the designation for the first team at Carnegie Mellon University [8].

National/governmental CERTs are a particular type of CERT playing an important role at a national level in supporting such cross-border coordination. They are primarily concerned with incidents affecting national information infrastructure. They can act as a contact point for sending and receiving cross-border requests concerning different types of information to help them detect, react and mitigate of an incident. The 2011 communication from the Commission on Critical Information Infrastructure Protection noted that as of March 2011, over 20 national/governmental CERTs had been established across Europe.

3.1. U.S. COMPUTER EMERGENCY READINESS TEAM

The DHS's U.S. Computer Emergency Readiness Team (US-CERT) leads efforts to improve the nation's cybersecurity posture, coordinates cyber information sharing, and proactively manages cyber risks to the nation while protecting the constitutional rights of Americans. US-CERT strives to be a trusted global leader in cybersecurity that is collaborative, agile, and responsive in a dynamic and complex environment [8]. As a domain expert in the enterprise side of the network, US-CERT focuses their expertise to securing the U.S. government from cyber events.

3.2. INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM (ICS-CERT)

ICS-CERT is a key component of the DHS strategy for securing ICS for U.S. infrastructure.[3] The primary goal of DHS's strategy is to build a long-term common vision where effective risk management of control systems security can be realized through successful coordination efforts [9]. ICS-CERT leads this effort by:

- Responding to and analyzing control systems-related incidents
- Conducting vulnerability, malware, and digital media analysis
- Providing onsite incident response services
- Providing situational awareness in the form of actionable intelligence
- Coordinating the responsible disclosure of vulnerabilities and associated mitigations

[3] DHS has designated 16 critical sectors in the U.S.

- Sharing and coordinating vulnerability information and threat analysis through information products and alerts.

ICS-CERT domain expertise resides on the cyber-physical aspects of U.S. critical infrastructure. As an organization recognized by the international community, ICS-CERT provides unique services and products to asset owners within the U.S. and international partners.

3.3. DESIRABILITY OF AN INTERNATIONAL NUCLEAR CERT

NSS documents developed by IAEA do not specifically state a need or requirement for a CERT or any similar body dedicated to cybersecurity support in a near real-time environment. Although the development of a CERT is not directly required by existing NSS documents, the desirability of a CERT-like entity to support member state nuclear cybersecurity requirements is supported by requirements identified in Section 1 and the increased ICS presence and exposure discussed in Section 2.

Section B of the *Nuclear Security Plan 2014–2017* lists a number of developments that occurred over the four year period of the implementation of *Nuclear Security Plan 2010–2013*. Lessons learned from these developments were listed in Section B.2 and considered while developing the current security plan. The following lesson listing adds emphasis to highlight factors foreseen as potential NS-CERT challenges (should one be established).

- As recognized in the NSS publications, the responsibility for nuclear security within a state rests entirely with that state. However, a nuclear security event or a weakness in nuclear security measures in one state has the potential to involve or affect other states, and there is a growing recognition among states that nuclear security is a global issue that needs to be addressed on a global basis.
- Potential adversaries have demonstrated an ability to plan their activities globally. Therefore, those who seek to prevent and mitigate criminal or intentional unauthorized acts with global aspects must plan for, and be prepared to participate in, a global response.
- Nuclear security involves entities in a state beyond the traditional agency constituency in the planning and execution of nuclear security activities. These include, for example, customs officials, administrators of medical facilities, border guards and law enforcement organizations. Feedback from the practical use of agency guidance will enable the sharing of best practices.
- The involvement of all member states in agency activities and initiatives relating to nuclear security is needed. Participation by their representatives and experts in the Nuclear Security Guidance Committee and in agency-sponsored activities can involve member states more closely and provide an opportunity for a greater sense of ownership in the development and application of nuclear security guidance documents as well as increasing their acceptance.

The experience gained by CERTs in the U.S. and throughout the world, as well as the lessons learned by the IAEA in developing *Nuclear Security Plan 2014–2017*, indicate the value of CERTs in general and the specific desirability of an NS-CERT. By drawing on the accumulated experience and know-how of existing CERTs and adapting it to identified IAEA requirements, it will be possible to develop the form, structure, and concept of operations of an NS-CERT.

4. FRAMEWORK FOR A NS-CERT

The list of IAEA lessons learned combined with general CERT operations and specific INL and DHS experience with a CERT, point-to-development framework to support to the establishment of an effective NS-CERT. That framework would include:

- **Nuclear Cybersecurity Information Sharing Agreement:** Identify and implement a mechanism to share sensitive nuclear cybersecurity information across multiple international organizations.
- **Nuclear Cybersecurity Requirements List:** Articulate and organize the disparate cybersecurity requirements submitted by Member States into a single nuclear cybersecurity requirements list.
- **NS-CERT:** Establish a single organization known as the NS-CERT that will be responsible for development of resident resources and capabilities to implement an effective, international cybersecurity emergency reporting and response program under authorities granted by Member States through the IAEA. In order to fulfill its assigned responsibilities, the NS-CERT should be comprised of at least the following three functional branches:
    - Nuclear Cybersecurity Analysis Group
    - Nuclear Cybersecurity Emergency Response Group
    - Nuclear Cybersecurity Forensics Group.

In order to establish and develop the level of technical capabilities and complexity to support establishment of a NS-CERT, the international community will need to leverage the resources and subject matter expertise that exist within each member state. An international NS-CERT will need to be a shared responsibility and commitment.

4.1. ORGANIZATIONAL RELATIONSHIPS

A logical assumption based on diversity of member states and international agreements is to have a CERT affiliated with IAEA. The place that the NS-CERT might hold within the IAEA structure remains to be determined; logically, it would be related to or subordinate to the Department of Nuclear Safety and Security (see FIG. 3). Although it is similar in nature to the Incident and Emergency Centre, there is enough difference in function and focus that a separate position under the Department of Nuclear Safety and Security might be formed.

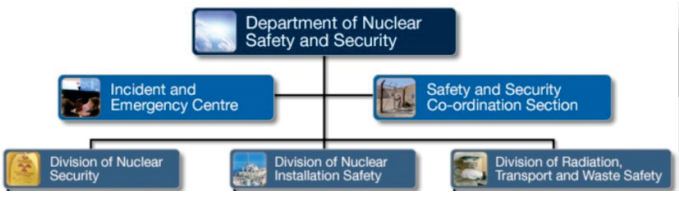

FIG. 3. IAEA Nuclear Safety and Security organization.

4.2. CYBERSECURITY INFORMATION SHARING AGREEMENT

The role of CERTs should be to report actionable information to end users that enables organizations to mitigate the cybersecurity risk to their operations. In order to accomplish this task, CERTs are required to work with researchers, I&C vendors, software developers, facility owners and operators, and organizations to develop mitigation measures that are implementable by interested parties. The results of these actions require information to be analyzed, put into operational context, and shared.

To have an effective CERT, information must be protected from potential actors that would cause harm and shared with end users so that they can reduce the risk from a malicious attack [10].

The legal structure necessary to establish and operate the NS-CERT will require a great deal of planning and advance coordination. The sensitive nature of information related to nuclear cyber-physical systems, their potential vulnerabilities, and potential threats to those systems dictates that proper safeguards and means of protection be established in an information sharing agreement. Additionally, means and methods to exchange information must be established to ensure security.

In 2011, IAEA launched the Unified System for Information Exchange in Incidents and Emergencies. This is a single unified website for national contact points and for International Nuclear and Radiological Event Scale national officers to report and exchange information on nuclear and radiological incidents and emergencies [11]. Building on the Unified System for Information Exchange in Incidents and Emergencies concept and the DHS ICS-CERT portal format, it would be possible to develop a NS-CERT portal, capable of providing general information to a broad group of subscribers and, at the same time, provide protected exchange of sensitive information.

4.3. CYBERSECURITY REQUIREMENTS LIST

The Nuclear Cybersecurity Requirements List will articulate and organize the disparate cybersecurity requirements submitted by member states into a single data base. Member states need to be solicited to advise the NS-CERT, or designated organization, of their perceived cybersecurity needs. These needs will be reviewed, evaluated, organized, and entered into an online database to serve as standing requirements to govern prioritization of NS-CERT activities and reporting.

4.4. CERT STRUCTURE AND OPERATIONS

Initially, the NS-CERT will be responsible for providing three primary types of cybersecurity services: (1) near real-time and term threat analysis and reporting, (2) emergency response (either remotely or jointly on the ground with member state entities), and (3) forensics.

Although this description of the NS-CERT speaks of a single organization, it must be understood that it may be advantageous to allow for a structure that is both virtual and distributed. For example, the Nuclear Cybersecurity Analysis Group might be located in Vienna, Austria, perhaps near to the Incident and Emergency Centre. The Nuclear Cybersecurity Emergency Response Group and the Nuclear Cybersecurity Forensics Group, on the other hand, might be collocated in different locations, convenient for rapid deployment in response to incidents. Despite the location, they would be tied together by redundant, secure communications paths and have ready access to teleconferencing and other real-time collaboration tools.

Information sources to supply the timely reporting of situational and technical data needed by NS-CERT will include the IAEA Incident and Emergency Centre (IEC), various CERTs throughout the world, and selected partners possibly to include organizations already participating in the Joint Radiation Emergency Management Plan. Each international organization may have links with the relevant authorities in its own member state for performing its usual functions.

The following graphic depicts a general view of the nuclear cybersecurity information sharing path. The path starts with information submitted by participating contributors, onward to the

cybersecurity threat analysis environment at NS-CERT, culminating in reporting to member states. Member states then pass the reporting to appropriate agencies and facilities. The graphic also shows the path for feedback and requirements from member states to NS-CERT.

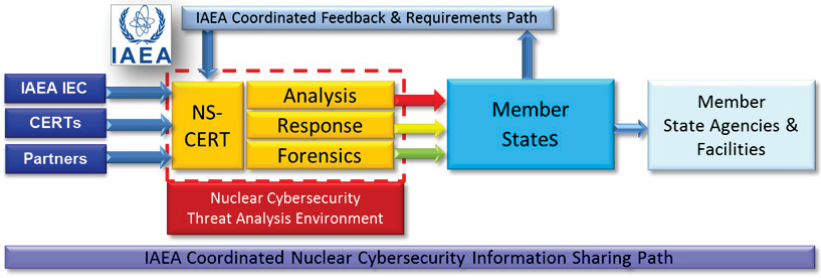

FIG 4. CERT information sharing model.

4.4.1. NS-CERT Cybersecurity Analysis Group

The purpose of the Nuclear Cybersecurity Analysis Group is to define, establish, and operate a center with the capability to monitor, filter, and analyze multiple cybersecurity information inputs and to provide near real-time situational awareness and threat assessment products to member states, member state entities, and other partners as requested by member states, and as required by the Nuclear Cybersecurity Requirements List and NS-CERT governing documents.

4.4.2. Nuclear Cybersecurity Emergency Response Group

The purpose of the Nuclear Cybersecurity Emergency Response Group is to maintain a cadre of nuclear cybersecurity experts (analysts, engineers, and forensic) to assist member state entities in resolving emerging cybersecurity incidents, either remotely or jointly on the ground with member state entities.

4.4.3. Nuclear Cybersecurity Forensics Group

The purpose of the Nuclear Cybersecurity Forensics Group is to establish a team of nuclear cybersecurity experts to develop the baseline knowledge necessary to understand the consequences and impact of cybersecurity in the nuclear context to include:

- How nuclear systems work and what process are being controlled
- The engineering purpose of systems (e.g., protection, safety, and security; software and hardware for management of data and information between enterprise and operations)
- Profile capabilities of malicious actors
- Analysis of malware in order to develop mitigation and organizational policies that address the dynamic nature of cybersecurity.

5. FILTERING, ANALYSIS, AND REPORTING IN SUPPORT OF NUCLEAR CYBERSECURITY

Following is a discussion of how the NS-CERT Cybersecurity Analysis Group would work to render actionable, near real-time cyber security analysis and reporting in support of IAEA member states based on monitoring and filtering of multi-source situational awareness and technical data.

The NS-CERT conducts multi-source fusion analysis using current (C) + term, trend, threat analysis (T^3A) methodology[4]. FIG. 5 depicts the two major and two minor analysis components of the C+T^3A methodology. The methodology incorporates the following elements:

- C+T^3A combines Current and Term Analysis to produce information to support operational Trend and Threat Analysis
- C+T^3A data sources range from fully open to highly sensitive and are analyzed in a multi-source fusion environment
- C+T^3A's goal is to disseminate actionable intelligence rapidly to IAEA member states.

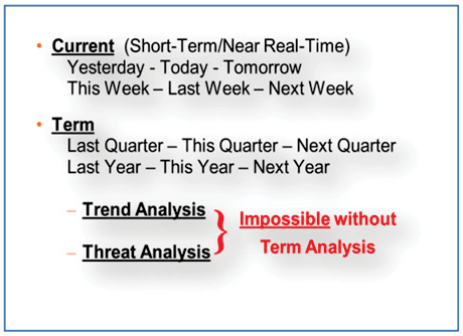

FIG. 5 C+T^3A methodology.

5.1. CURRENT ANALYSIS

The analysis function provides several levels of insight into threat awareness as it pertains to NPP and nuclear safeguard processes. In near real-time, analysts examine raw and summarized data from a wide variety of information sources and review, collate, categorize, and evaluate information and determine relevance based on essential elements of information to make determinations about potential incidents. This critical analysis activity not only identifies many of the incidents to which NS-CERT must respond, but also helps to characterize and prioritize them in terms of their level of threat, determination that an attack is taking place, the type of attack being employed, and the vulnerability of the targeted I&C system (this activity is iterative and continuous).

The Cybersecurity Analysis Group reviews all reported information upon receipt and conducts analysis based on best practices, technical tools, and defined processes and procedures. It performs information aggregation activities, pulling together information from a variety of sources and other NS-CERT activities (e.g., forensic analysis) to assess a potential incident's scope and possible impact to nuclear sector assets. This analysis guides the short-term response and mitigation activities within the NS-CERT.

5.2. TERM ANALYSIS

The Cybersecurity Analysis Group separately reviews information sourced through its connections to appropriate resources and member states. Analysis of this information, preprocessed and aggregated from a variety of sensitive sources, is reviewed, collated, categorized, and evaluated to determine relevance based on the Nuclear Cybersecurity Requirements List. It allows the NS-CERT to assess potential long-range threats and their impact to nuclear sector assets. This analysis guides long-term response and mitigation strategies within the NS-CERT.

[4] The C+T^3A concept was presented November 2011 at "Protecting the Nation's Bulk Power and Distribution System from Emerging Threats" workshop. INL's ICS-Mission Support Center proposed development of a cyber-threat matrix for the electric sector and a means for dissemination of actionable intelligence to electric sector stakeholders.

Generating actionable mitigation products from raw data requires a rigorous approach to information management, the careful categorization of composite product, and close attention to the acquisition, retention, and retrieval of information stored in cumulative technical and historical databases.

5.3. THREAT ANALYSIS

The Cybersecurity Analysis Group conducts fusion and analysis of information derived from the various acquisition sources to determine active, impending, potential, and insubstantial threat. Both current and term threat analysis are also supported through access to information stored in term analysis technical and historical databases. Threat analysis is conducted in accordance with the general threat principles discussed in Section 3.3.

5.4. TREND ANALYSIS

The Cybersecurity Analysis Group conducts fusion and analysis of information derived from the various acquisition sources to determine trends in development of threat capabilities and intent. It also monitors advanced changes in nuclear sector activities to understand how those factors might influence the perceptions or activities of threat actors. Trend analysis is highly dependent upon quantity and quality of information stored in term analysis technical and historical databases.

6. CONCLUSION

Although the NSS documents do not call out a specific need or requirement for a CERT or any similar body, the international community is awakening to an increased level of cybersecurity threats potentially targeting nuclear facilities. Drawing from the NSS documents and lessons learned from development of *Nuclear Security Plan 2014–2017*, this paper presented background information summarizing the perceived need for a CERT-like entity to support the international community's cybersecurity prerequisites to ensure that organizations are protected from eminent cyber threats. This paper also provided a conceptual framework for establishing a CERT-like entity that would perform multi-source analysis resulting in near real-time reporting of actionable nuclear cybersecurity products to member states. That entity would also perform cybersecurity forensics and respond to emerging incidents in accordance with a list of mutually agreed upon nuclear cybersecurity requirements. That entity would be the NS-CERT.

7. REFERENCES

[1] IAEA, “Nuclear Security Plan 2014-2017,” in *Report by the Director General, IAEA Board of Governors Conference*, 2 August 2013.

[2] IAEA, “IAEA Nuclear Security Series No. 13 (NSS-13), Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities,” Vienna, 2011.

[3] IAEA, “IAEA Nuclear Security Series No. 17 (NSS-17), Computer Security at Nuclear Facilities,” Vienna, 2011.

[4] IAEA, “IAEA Nuclear Security Series No. 19 (NSS-19), Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme,” Vienna, 2013.

[5] Gasper, P. D., “Cyber Threat to Critical Infrastructure 2010-2015: Increased Control System Exposure,” Idaho National Laboratory, 24 September 2008. [Online]. Available: http://usacac.army.mil/cac2/cew/repository/papers/Cyber_Threat_to_CI.PDF.

[6] ICS-CERT, “ICS-CERT Year in Review, Industrial Control Systems Emergency Response Team 2014,” [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/documents/ICS-CERT%20YIR%202014.pdf [Accessed 20 April 2015].

[7] Dudenhoeffer, D., “Office of Nuclear Security Cyber Security Programme,” [Online]. Available: http://www.iaea.org/NuclearPower/Downloadable/Meetings/2013/2013-05-22-05-24-TWG-NPE/day-2/4.cyber_security_introduction.pdf. [Accessed 16 February 2015].

[8] “Computer Emergency Response Team,” [Online]. Available: http://en.wikipedia.org/wiki/Computer_emergency_response_team. [Accessed 16 February 2015].

[9] US-CERT, “About Us,” [Online]. Available: https://www.us-cert.gov/about-us. [Accessed 2 March 2015].

[10] IAEA, “Security of Nuclear Information,” [Online]. Available: http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1677web-32045715.pdf. [Accessed 4 April 2015].

[11] IAEA, “Unified System for Information Exchange in Incidents and Emergencies (USIE),” [Online]. Available: http://www-ns.iaea.org/downloads/iec/usie.pdf. [Accessed 4 March 2015].

[12] IAEA, “Unified System for Information Exchange in Incidents and Emergencies (USIE),” [Online]. Available: http://www-ns.iaea.org/downloads/iec/info-brochures/13-27011-usie.pdf. [Accessed 4 March 2015].

AUTHORS' BACKGROUND:

Mr. Julio Rodriguez was responsible for managing and leading the team that developed the non-nuclear I&C cybersecurity focus at Idaho National Laboratory. This included the development of the Department of Energy National Supervisory Control and Data Acquisition Test Bed Program in 2003 being and establishing Department of Homeland Security Control Systems Security Program in 2004, and the Industrial Control Systems – Computer Emergency Response Team in 2007. Currently Mr. Rodriguez supports the Department of Energy National Nuclear Security Administration cyber security programs.

Mr. Peter Gasper is the Senior Critical Infrastructure Security Analyst for National & Homeland Security at Idaho National Laboratory, specializing on critical infrastructure protection, and industrial control systems networks. He developed and established analysis procedures at the Department of Homeland Security Industrial Control Systems-Computer Emergency Response Team. He also established a private information security consulting service and authored a weekly newsletter on international cyber technology developments for United Press International. As Senior Geopolitical Analyst for a network security company, he authored assessments of threats posed by international hacking and cyber-criminal elements.