VCDNP
Vienna Center for Disarmament and Non-Proliferation

The Cyber-Nuclear Security Threat: Managing the Risks

January 2017

by Vesselin Giaurov*

*The views expressed in this article are the author's and do not necessarily represent the VCDNP.
*Cover image: Illustration by Julian Stankulov - Artist

The Cyber-Nuclear Security Threat: Managing the Risks

Acknowledgements

A large number of people generously contributed with their expertise to this research paper. In particular, I would like to thank:

Dr. Laura Rockwood, Executive Director of the Vienna Center for Disarmament and Non-proliferation (VCDNP)

Jenny Nielsen, Senior Research Associate at the VCDNP

Sitara Noor, Senior Research Associate at the VCDNP

Sven Weizenegger, Senior Vice-President - Security at Kreditech Holding SSL GmbH

Vienna Center for Disarmament and Non-proliferation – VCDNP (www.vcdnp.org)

EU Non-Proliferation Consortium (www.nonproliferation.eu)

I would like to express my acknowledgment for their aspiring guidance, invaluably constructive criticism and friendly advice during the project work. I am sincerely grateful to them for sharing their truthful and illuminating views on a number of issues related to the project.

Content

I. Introduction

Looking into the future has always provoked humans' creativity, imagination and perceptions. Looking at humans' perceptions about the world one can notice that we have entered a period of interplay between the real and the virtual world. In the future, this cyber-physical phenomena will influence all aspects of our lives and it is necessary to understand the cyber security threat landscape in order to ensure that these phenomena are properly addressed. Broadly speaking, the future of nuclear security depends on how we manage the risks and control the threats. Cyberspace is part of everything surrounding us and, as such, must be secured properly. Although there already exist numerous pledges and commitments about cyber security, action is still lacking with respect to many of them.

A significant question remains unresolved, undeveloped and, to some extent, unrecognized: the cyber risks threatening cyber-nuclear security.

What do cyber technologies, cyberspace and cyber security have to do with nuclear security? All impact the ability to manage, access, store and process data received from the physical and chemical processes that occur in a nuclear facility.

This report analyses cyber security as it relates to nuclear security. The objectives of this analysis are: to create awareness of the importance of incorporating cyber security as a fundamental part of overall security for nuclear facilities at all stages of the nuclear fuel cycle and to provide recommendations and possible solutions for developing and maintaining a high level of cyber security at nuclear facilities that conforms to national and international security objectives.

The report aims to address the range of technical, policy and legal challenges, as well as practical recommendations based on advice and best practice derived from the digital financial industry.

II. Understanding the terminology

Defining the terms "cyber", "cyberspace" and "information and communication technologies" is key to proceeding with any discussion of cyber security, cyber risks and cyber attacks. This task is complicated by the fact that, even among cyber experts, there

is no consensus on such definitions. The definitions identified below, however, reflect, in the view of the author, reasonable definitions.

For the purpose of this analysis, the term "cyber" is used to refer, collectively, to information technology and computer systems, data processing, electronic communications and virtual reality.

"Cyberspace" in turn is used to refer to where virtual reality resides, a fast growing and evolving virtual space with great potential and innumerable applications.

"Information and communication technologies" or "ICTs" refers to an interactive digital environment used to store, modify and exchange data using computer networks. More precisely, ICTs encompass a "complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form".[1]

III. Understanding the threat

Over the last few years, cyberspace has become one of the most important and rapidly developing technology domains. It is also becoming more and more recognizable in its negative connotations. Mobile computing, Big Data, cloud computing, the "Internet of Things", artificial intelligence and social media are further complicating the threat environment.

Cyber risks should be considered one of the most rapidly evolving global threats today. ICTs have become a fundamental part of daily life for the majority of the world's population, as well as a basis for innovation and economic growth. In the nuclear field, these technologies have enormous benefits, but they also entail substantial risks, as the information they contain or convey can also be accessed and used for criminal purposes.

The number, magnitude, and impact of cyber attacks are on the rise, as is the level of concern about the high vulnerability of the Internet, a tool on which practically every economic activity relies. The Internet was designed as an essentially open platform,

[1] ISO/IEC JTC 1, Joint Technical Committee of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC 27032:2012), 2012.

because its creators did not anticipate that it would be used to offer a wide range of critical services requiring tighter security.[2]

Preventing cyber attacks has become an important and strategic challenge for states, a national security issue that could potentially impact not only the nuclear sector, but on all societal sectors. The possibility of deliberate or unintended cyber attacks executed by state or non-state actors raises concerns about current and future risks in the cyber domain. Potential risks include:

- the risk of disruption in facility operation;
- damage to physical facilities;
- espionage (commercial and political);
- interference with critical infrastructure ("CI")[3];
- potential radiological incident;
- erosion of public confidence in nuclear energy; and
- theft of nuclear or other radioactive material.

Moreover, the lack of information and accurate attribution in the event of successful cyber attacks could spark conflict between and/or among states, whether bilateral, regional or international. Even more seriously, such an attack could potentially develop into a conflict between or among nuclear-weapon states.

With developments in ICTs come increasing cyber vulnerabilities. Cyber attacks could be very complex and dynamic. Over time, malware can go through extensive evolution and be reused, resulting in new vulnerabilities. Cyber attacks involving malware can often reach beyond the target for which they were intended, easily spreading into public networks. Such malware can fall into the hands of different users and can be used for the development of other new malware.[4]

---

[2] Javier Solana, BBVA Open Mind, European Foreign Policy and Its Challenges in the Current Context, 2016, https://www.bbvaopenmind.com/wp-content/uploads/2016/01/BBVA-OpenMind-Javier-Solana-European-Foreign-Policy-and-Its-Challenges-in-the-Current-Context.pdf.

[3] "Critical infrastructure" refers to essential services and sectors that are the backbone of every nation's economy, security and health. Overall, there are 16 sectors, which are considered vital for the functioning of a society and economy. See https://www.dhs.gov/critical-infrastructure-sectors.

[4] Alexander Klimburg, National Cyber Security Framework Manual, CCDCOE, 2012, https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf.

Cyber attacks in connection with nuclear facilities have already happened, some of which have been highly complex. Some examples of such cyber attacks include:

- worm infection of the Davis-Besse Nuclear Power Plant (NPP) in 2003;[5]
- Stuxnet in 2009;[6]
- cyber espionage and blackmailing campaign against the operator of the Korea Hydro and Nuclear Power Plant in 2014;[7]
- attacks on the ThyssenKrupp steel mill in Germany in December 2014;[8]
- energy blackouts in Ukraine in December 2015 that affected 225,000 customers[9] and allowed attackers to control the grid's industrial control systems (ICS) and supervisory control and data acquisition (SCADA) components; and
- worm infection of the Gundremmingen nuclear power plant in Germany in April 2016.[10]

Despite the fact that ICTs are widely accessible, other obstacles remain that limit the ability of a terrorist organization or other non-state actor to cause substantial damage or disruption in nuclear installations. Some experts argue that "terrorism related to nuclear cyber security is an illusion. Not only it is difficult to find the right people with the right skills, expertise and experience, it is difficult to acquire regular on site information and to

---

[5] Brent Kesler, Strategic Insights, The Vulnerability of Nuclear Facilities to Cyber Attack, Volume 10, Issue 1, 2011; http://large.stanford.edu/courses/2015/ph241/holloway1/docs/SI-v10-I1_Kesler.pdf; "The Slammer worm infected computer systems at the Davis-Besse nuclear power plant near Oak Harbor, Ohio. The worm traveled from a consultant's network, to the corporate network of First Energy Nuclear, the licensee for Davis-Besse, then to the process control network for the plant. The traffic generated by the worm clogged the corporate and control networks. For four hours and fifty minutes, plant personnel could not access the Safety Parameter Display System (SPDS), which shows sensitive data about the reactor core collected from coolant systems, temperature sensors, and radiation detectors—these components would be the first to indicate meltdown conditions."

[6] The world's first cyber weapon, code-named "Olympic Games" and later called "Stuxnet" by computer security researchers.

[7] In 2014, an unknown individual or group posted online designs and manuals of plant equipment owned by Korea Hydro and Nuclear Power Co (KHNP).
http://www.bbc.com/news/world-asia-30572575

[8] R.M.Lee, M.J.Assante, T.Conway, German Steel Mill Cyber Attack, Industrial Control Systems SANS, 2014.
https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf; "According to the report of the German government's Bundesamt für Sicherheit in der Informationstechnik (BSI) (translated as Federal Office for Information Security) the adversary was able to cause multiple components of the plants network system to fail. This specifically impacted critical process components to become unregulated, which resulted in massive physical damage."

[9] Dustin Volz, U.S. Government concludes cyber attack caused Ukraine power outage, Feb 25, 2016, http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K.

[10] "The malware can steal login credentials and allow a remote attacker to access the cracked computer." https://www.rt.com/news/341083-germany-gundremmingen-plant-virus/

bypass all different security levels in nuclear facilities."[11] These experts would argue that the real threat is state-on-state cyber attack.

However, the threat posed by state-on-state attacks may be more manageable to overcome and prevent, because the process for negotiations, the mechanisms in support of these processes and the possibilities for finding a solution are a lot more facilitated between states.

Nevertheless, there is currently a lack of international mechanism for preventing and containing cyber conflicts. The current system of international law is not adapted to the challenges and threats posed by the use of cyber technologies for military-political purposes.

International security is facing new challenges from nuclear cyber threats. Understanding the cyber threat landscape is necessary to be able to address such threats properly.

A. Managing cyber risks through effective technical measures

Improving cyber security involves a combination of complex technical, legal, economic and policy instruments. One of the initial technological problems in cases of sophisticated cyber attacks is the difficulty in identifying with high precision the real perpetrator of cyber attacks (attribution).

One of the most common practices in tracing and finding more information about the initiator of the attack is through Internet Protocol ("IP") address detection. It is, however, not sufficient to trace the perpetrator of an attack. There are multiple techniques for obscuring the origin of the perpetrator of a cyber attack, including the use of no-log virtual private network (VPN) services, virtual machines, and by controlling domain name system (DNS)[12] information leaks.

All these techniques can be used against the digital control systems of nuclear facilities.

The advanced control systems offer effective management in all phases of nuclear enterprises work, but they are the ones increasing the risks and the vulnerabilities. There has been good technical progress in automation control and security with respect to

[11] Sven Weizenegger, SVP of Cyber Security at Kreditech, Hamburg, 03 June 2016.

[12] The Domain Name System (DNS) is a decentralized hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. It associates various types of information with domain names assigned to each of the participating entities. https://en.wikipedia.org/wiki/Domain_Name_System.

current digital operating systems in the nuclear industry. However, at the same time, the ICT gaps, such as a lack of effective human resource management and gaps in information sharing, communication, quality control, supply chain security and the level of network security, have to be properly addressed.

One of the systems for advanced process control that has been widely discussed recently is the supervisory control and data acquisition system ("SCADA").[13] Digital modules such as SCADA, which include programmable logic controllers (PLCs)[14] and remote terminal units (RTUs),[15] today operate and control many critical systems. For example, in the nuclear industry, coolant systems, centrifuges, and power generators are digitally controlled. SCADA managing electronic modules are a closed system with the same input and output of data - which means that they are not as complex as IP systems. Normally a more simple system is characterized by less failure opportunities - it is more fault tolerant. Although SCADA is not a very complex controlling unit, it still shows some weak points.

On the other hand, the current expansion of internet-connected automation and digital control systems (frequently referred to "smart industrial management systems') is allowing optimization of plants' safety and security, real-time energy optimization, automated controls, predictive maintenance, statistical evaluation and measurements to maximize reliability. Such systems are integrated in many CI networks.

CI networks started becoming connected to the Internet in the early 2000s. SCADA systems and other industrial software applications were brought online, allowing smarter business process management. Big data has been adapted to ensure more efficient operation of industrial smart grids. The "Internet of Things" and "Internet of Everything" are rapidly bringing industries towards a revolution in process control

---

[13] SCADA is a system for remote monitoring and control that operates with coded signals over communication channels. https://en.wikipedia.org/wiki/SCADA.

[14] Programmable logic controller or "PLC", is a digital computer used for automation of typically industrial electromechanical processes, such as control of machinery on factory assembly lines, amusement rides, or light fixtures. PLCs are used in many machines, in many industries. https://en.wikibooks.org/wiki/Introductory_PLC_Programming.

[15] Remote terminal unit (RTU) is a microprocessor-controlled electronic device that interfaces objects in the physical world to a distributed control system or SCADA (supervisory control and data acquisition) system by transmitting telemetry data to a master system, and by using messages from the master supervisory system to control connected objects.
Gordon R. Clarke, Deon Reynders, Edwin Wright, Practical modern SCADA protocols: DNP3, 60870.5 and related systems Newnes, 2004 ISBN 0-7506-5799-5 pages 19-21, https://en.wikipedia.org/wiki/Remote_terminal_unit.

practices, where each "smart" sensor, actuator or detector installed at the facility is connected online, collects and supplies data online to the enterprise server.[16] This allows objects to collect and exchange data (provided by a large number of networked sensors), to be sensed and controlled remotely across network infrastructures.

Digitalized operating systems and smart connected digital systems are generating data that is helping us to understand better the processes in industrial systems, but must also be carefully managed and secured.

The most effective and cost-efficient route to improved cyber security – to make the IT infrastructure more resistant to hostile cyber operations – is the development of secure code. The less vulnerable the computer code, the less systems can be manipulated, whether for monetary gain, espionage or system manipulation. Yet, building a legal economic and policy framework to achieve this objective has eluded the security community for over two decades.[17]

Thus, policy and economic decisions for improving cyber security will allow development of better technological solutions for attributing and handling cyber threats.

B. Managing cyber risks through legal measures

The establishment of international and domestic legal rules and regulations could also constrain offensive operations in cyberspace.

Cyber security is a strategic political and governmental issue, a matter of national and international security. However, there is limited common agreement among states on the risks or their mitigation. Nor is there consensus on the terminology and definitions associated with cyber security.

There should be agreement on norms regulating cyber activities with respect to critical nuclear infrastructures. Norms and agreements should directly reflect the degree of risk that disruption to critical infrastructure services may pose to society and the economy.

---

16 World Economic Forum, PIR Center, Cybersecurity of Civil Nuclear Facilities: Assessing the Threat, Mapping the Path Forward, June 2016, http://www.pircenter.org/media/content/files/13/14664952850.pdf.

17 Liis Vihul, The Tallin Papers, CCDCOE, The liability of software manufacturers for defective products, 2014, https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_02.pdf.

In comparing cyber weapons and nuclear weapons, it is worth noting that nuclear weapons production and development still remain state governed. In contrast, cyber weapons are more accessible, not only to states, but also to criminal organizations and terrorist groups. Regulating cyber attacks through different legal mechanisms and norms would minimize the risk of eventual cyber attack.

There are several legal frameworks in addition to the laws of war that are to some extent relevant to regulating cyber attacks. These include:

International law of countermeasures regulates self-defense and how states may respond to violations of international law that do not rise to the level of armed attack. Here, the difficulty is identifying the state responsible for the attack. Before a state may use active defense as a countermeasure, it must identify accurately the state responsible for the act (and the network and computer from which the attack originated) and determine that an internationally wrongful act caused harm. Countermeasures are inherently useful for addressing cyber attacks that do not rise to the level of an armed attack. To be effective, the countermeasure must be costly enough to the perpetrator to compel termination of the unlawful act. Countermeasures also to respond to the actual act and need to be temporary - once the cyber attacks stops, the countermeasure must be stopped as well.

International legal regimes that directly regulate some elements of cyber attacks, such as those created by NATO, the Shanghai Cooperation Organization (SCO), the Council of Europe, and the United Nations, as described below.

- The Cooperative Cyber Defence Centre of Excellence is a NATO creation dedicated to developing long-term NATO cyber defence strategy. A group of experts assessed how the existing law of armed conflicts and international humanitarian law are applicable to cyber space, which led to the 2013 publication of the *Tallin Manual on the International Law Applicable to Cyber Warfare*.
- The SCO has taken steps toward building future cooperation for international information security.[18]

[18] The International Code of Conduct for Information Security (the "Code") is an international effort to develop norms of behavior in digital space. In 2009, the Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security (Yekaterinburg, 16 June 2009) was concluded. On 12 September 2011, four members of the SCO submitted a Draft International Code of Conduct for Information Security to the United Nations General Assembly. This initial group was expanded to six members in 2015, when it submitted a second Draft to the UN General Assembly.

- The Council of Europe has provided direction on issues with regard to crimes in cyberspace.[19]
- The United Nations has taken initial steps towards bringing together the global cyber powers (United States, China and Russia) to address the main cyber security issues and to submit recommendations for confidence-building measures for cyber security and stability.[20]

All steps taken by these organizations demonstrate increasing interest in regulating the cyber domain. However, many aspects of cyber crime have yet to be adequately addressed.

States' domestic laws – domestic policies are of great importance in establishing cyber-secured societies. Yet, domestic laws and policies cannot achieve solutions applicable to global cyber challenges. Addressing global cyber challenges will require global cooperation. Domestic laws are not designed with the purpose of regulating cyber attacks, and are therefore inadequate to address this issue. The scope of the cyber threats is global; the solutions should be developed at an international level.

Definitions regarding cyber attack, cyber crime and cyber warfare should be adopted by the international organizations in the context of a comprehensive binding treaty, a non-binding declaration or declarations or through independent agreements, which could form the foundation of future cooperation and dialogue. This could serve as a good starting point for developing a more comprehensive international treaty in the future.[21]

The key to solving legal challenges in connection with cyber is to ascertain how challenges posed by ICTs can be addressed through legal measures. The law of armed conflicts should be adapted to apply to the cyber domain. In periods of armed conflict, any cyber attacks on nuclear critical infrastructure should be prohibited: massive electrical grid failures, including potential failures of nuclear installations, can be followed by humanitarian crises.

---

[19] Convention on cybercrime: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
Agreement from 09 June 2016 on improving criminal justice in cyberspace: http://www.consilium.europa.eu/en/press/press-releases/2016/06/09-criminal-activities-cyberspace/.

[20] United Nations CBMs (p.135-136): https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_Ch7.pdf.

[21] Oona Hathaway, Yale Law School, The law of cyber-attack, January 2012, http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=4844&context=fss_papers.

It should be noted that "…in most cases, existing laws for armed conflict can be applied to cyber attack, but there are areas of ambiguity involving the violation of third party sovereignty, the use of cyber attacks by terrorists, and the amount and nature of damage from cyber attack that could be interpreted as an act of war. Some operational issues, such as the amount of prior assessment of collateral damage required to make an attack consistent with the laws of war are also unclear."[22]

Disruption of nuclear critical infrastructure could also cause severe economic losses and civil disturbance, and could lead to increased tension between states and regional or global armed conflicts. One example of international cooperation in the search for adequate legal measures for improving cyber security is the 2016 Nuclear Security Summit (NSS 2016) in Washington DC, which promoted the establishment of confidence building measures (CBMs) by the Organization for Security and Co-operation in Europe (OSCE). Both initiatives have great potential for improving international cyber security in the nuclear sector.

The 2016 NSS highlighted the relationship between nuclear security, information security and cyber security with respect to nuclear infrastructure. As Russian scholar Alena Makhukova notes "in 2012, 29 participants of the Summit joined the 'Gift Basket'[23] on cyber security, a commitment to participate in two international workshops held by the UK on this topic in 2016. The workshops are designed to enable the states and their nuclear sectors to receive good practice in managing risks to industrial control systems in nuclear sites, as well as to examine the impact of using information technology in managing safety and security aspects of plant control systems".[24]

At the 2016 NSS, many of the participating states declared the measures they had taken to strengthen cyber security and improve existing cyber security measures. For example, Australia, the Czech Republic, Finland, Germany, Hungary, Japan, the Netherlands and

[22] James Lewis, Center for strategic and international studies, A note of the laws of war in cyberspace, April 2010, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/100425_Laws%20of%20War%20Applicable%20to%20Cyber%20Conflict.pdf.

[23] On this link is located the Joint Statement on Cyber Security and the 2016: Gift Basket on cyber security of industrial control and plant systems at nuclear facilities April 2016, http://www.nss2016.org/document-center-docs/2016/4/1/joint-statement-on-cyber-security.

[24] Alena Makhukova, Cybersecurity of Nuclear Infrastructure at the Nuclear Security Summit 2016, CyberPulse #2 (20), June 2016, http://www.pircenter.org/en/articles/2023-cybersecurity-of-nuclear-infrastructure-at-the-nuclear-security-summit-2016.

the Republic of Korea declared that they had replaced and/or renovated old components related to cyber security at nuclear facilities.

With regards to strengthening national legislation on cyber protection of nuclear infrastructure, Canada, the Czech Republic, Finland, France, Hungary, the Netherlands, the Republic of Korea, Spain, Switzerland and the United Arab Emirates stressed that they were planning to undertake such measures in the near future. Some countries had already implemented these measures., such as Belgium, India and Singapore, which had established new regulatory agencies for cyber security (including agencies for regulating infrastructures).

More than 20 states referred to actions and achievements in efforts to counter cyber threats against nuclear infrastructure in their NSS National Progress Reports.

Another significant practical step to enhancing transparency, as well as reducing misperception and escalation between states, are the OSCE CBMs. The CBMs include provisions for communication and information sharing at the governmental and expert level and for the use of the OSCE as a platform for exchanging best practices, with the aim of increasing inter-state cooperation and stability. The CBMs aim to reduce the possibility for conflict between states stemming from the use of cyber technologies.

OSCE activities with regard to cyber and ICTs are primarily focused on counter-terrorism. However, the OSCE started working on CBMs with regard to cyber, which means that the global community is recognizing the possibility of state-to-state cyber warfare. The OSCE has a long tradition of CBMs with regard to nuclear weapons. So the experience in nuclear weapons CBMs could be applied by States and facilitated by the OSCE.

IV. Mitigating the vulnerabilities

Cyber is big and growing and future cyber attacks will likely be more sophisticated. Therefore urgent measures are needed, including the enhancement of both offensive and defensive capabilities against cyber attacks directed at critical nuclear infrastructure.

There are many measures that could be applied in achieving better cyber security in nuclear facilities. Some of the following recommendations could be implemented as initial steps in improving cyber security. More importantly, those steps could be the

starting point in acknowledging cyber reality and accepting the importance of improving cyber security as part of future technological developments.

One way to counter threats to ICTs is by introducing organizational and technical improvements. In prioritizing improvements to cyber security, Howard Schmidt argues: "education, information sharing and better defense systems rank high."[25] This includes efforts to train more security professionals and have governments share more information with the private sector. "One thing we are looking at is how do we make sure that the private sector has the information it needs from the government," Schmidt said. According to Schmidt "The government must also be active in reducing its own vulnerabilities."

Furthermore, Schmidt argues that "we can't sit there and be waiting for the next intrusion attempts to take place," He said, "We need to become stronger in what we are doing so we are better able to resist the things that are being thrown at us."[26]

EDUCATION – the importance of the human factor

Education is key, because the human factor is fundamental to improving cyber security and because human activity introduces vulnerabilities in cyberspace. Examples of such vulnerability include: weak passwords; poor IT knowledge; and overreliance in computer systems. Such vulnerabilities are often exploited by malware and, if successful, can lead to infected computer systems. Creating awareness about the linkage between nuclear and cyber, how these systems work together and how they can be managed, is of a great importance. Other measures for improving cyber security range from software to physical solutions. Among the main considerations is how we manage the information, how we access, process, store, analyze and share it.

INDICATOR OF COMPROMISES – rapid communication and information sharing

In terms of information sharing, incident handling processes, such as the indicator of compromises ("IOC") software platforms, have already been developed. IOC platforms are considered the primary tool in developing cyber defense systems. Rapid communication and sharing of pertinent threat information in the current threat

[25] Ryan Singel, White House Cyber Czar: 'There Is No Cyberwar', April 2010, https://www.wired.com/2010/03/schmidt-cyberwar/.
[26] Ryan Singel, White House Cyber Czar: 'There Is No Cyberwar', April 2010, https://www.wired.com/2010/03/schmidt-cyberwar/.

environment is a key factor in detecting, responding and containing targeted attacks. IOC solutions can be useful not only for any industry, but especially across all critical infrastructure sectors.

Reliable statistics on cyber security incidents and purposeful attacks are not available. Detailed statistics combined with in-depth analysis would be beneficial for the operators from all types of critical infrastructures.

Organizations need to be able to communicate how to detect attackers on their networks and hosts using a machine digestible format that removes human delay from intelligence sharing.[27] This is the benefit of IOC platforms – facilitating and reducing the time needed for communication between stakeholders in reporting, detecting and analyzing information derived from cyber attacks.

"Using data converted to these standard formats can help security practitioners rapidly identify and access current threats, and determine how they act, who is responsible, and what course of action is needed."[28]

Examples of IOCs include: unusual account behaviors; unusual network traffic; strange network patterns; anomalies in privileged user account activity; login anomalies; increases in database read volume; suspicious configuration changes; unusual DNS requests; and Web traffic showing non-human behavior.

Documenting IOC and sharing information will allow industry and governments to improve incident response and computer forensics. For this reason, efforts are being made by several private companies to standardize IOC documentation and reporting practices.[29]

Governmental organizations could also benefit from accessing and sharing cyber threat intelligence with the industry by joining open source IOC community.

[27] Open framework for sharing threat intelligence, http://www.openioc.org/.
[28] Richard Struse, United we stand: Protecting against cyber threats with standards for sharing, The Organization for Economic Co-operation and Development (OECD), Internet Technical Advisory Commitee (ITAC) News, July 2015, https://www.internetac.org/archives/2328.
[29] Mandiant, a FireEye company, and OASIS are working on open-source sharing platforms like STIX, TAXII and OpenIOC.

LIABILITY – establishing quality standards

Not only software applications are prone to cyber attacks. Hardware is as well. A further step in cyber security development is addressing software and hardware vulnerabilities. The need for standardization and certification protocols for software and hardware applications has been recognized in the nuclear sector. Validation requirements for assurance and confirmation that software and hardware systems meet all specified requirements should be increased and specified for characteristics specific to nuclear facilities.

All software and hardware applications need to operate smoothly and fulfill all required functions, producing an acceptably low number of failures in operation. For that reason, implementation of strong rules for standardization and certification are necessary.

From the point of view of cyber security, nuclear installations, facilities and industries are no different from any other industrial sector, except that the safety requirements are among the most demanding.[30]

Establishing quality standards, using certified products and verification and validation[31] of the operation of these products are part of the development of any quality assurance (QA) process.

SUPPLY CHAIN SECURITY – enhance quality control

Supply chain risks are escalating as supply chain security is becoming increasingly difficult. Given this challenge, there is a dire need for the initial cyber security budget to be expanded in order to enhance quality control. An organization cannot be sure from where a risk will evolve. That is why supply chain security is an increasingly important challenge for implementation.

---

[30] Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control, the International Atomic Energy Agency (IAEA), Technical report series No. 384, 1999, http://www-pub.iaea.org/mtcd/publications/pdf/trs384_scr.pdf.

[31] Verification and validation (V&V) are means by which the product is checked, and by which its performance is demonstrated and assured to be a correct interpretation of the requirements. A continuous process of V&V must be actively applied throughout the software development cycle. V&V includes a strong element of checking, and leads to remedial action. By contrast, QA ensures that a suitable management process has been specified, that the development process conforms to the requirements of basic standards and that the process specified is followed, p.17, http://www-pub.iaea.org/mtcd/publications/pdf/trs384_scr.pdf.

Cyber supply chain risks affect sourcing, vendor management, supply chain continuity and quality, transportation security and many other functions across the enterprise and require a coordinated effort to address these challenges. [32]

Central processing units (CPUs) are mainly manufactured in Asia, and then shipped all over the world. Monitoring the supplies could be a solution, but it would be expensive and difficult to trace all hardware parts. Adequate financial support for cyber security needs to be secured in order to enhance quality control. Using good quality components, instead of using poor quality components, is also crucial for securing digitalized high-risk applications such as nuclear installations. Consequently, strong security supply chain policies should be adopted.

Sven Weizenegger expanded on this idea: "Security control could be illustrated as [a] barrier or garage door – The door is recognizing a particular car and then giving it access to enter inside, but not checking what is inside. We trust the garage door, but we are not sure about the quality of the content that is coming in. We are assuming that when the car is allowed to enter through the garage door it is safe. But in reality [especially] in the nuclear industry […] the high quality of each hardware component and each software product is of a great importance."[33]

Cyber security is needed in all phases of the supply chain. Areas of concern include not only the quality of the products, but how the information about a particular product is stored. Critical questions need to be asked and answered in order to help strengthen cyber security: Who should be permitted to have access to software code? Who has written the code? Who is allowed to order that same product?

TRUST BOUNDARIES-Essential in establishing network security

Another step in managing cyber risks is identifying trust boundaries, a critical step in formulating cyber security for nuclear applications. No data from untrusted sources should be run through the security software.

Threat modeling, together with a more complete understanding about the trust boundaries and data flows that exist within a given system, is essential to identifying

[32] Conference material, Best Practices in Cyber Supply Chain Risk Management, National Institute of Standards and Technology (NIST), http://www.nist.gov/itl/csd/upload/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf.

[33] Weizenegger, personal communication, 3 June 2016.

relevant threats. Trust boundaries are based on assets and processes inside applications. Threat actors and vectors are classified based on their motivation and access to resources, by the IT security department. Together, they can be used to identify, classify and mitigate threats.

To put it simply, threats originate from untrusted sources. Therefore, defining trust boundaries is essential to establishing network security. Known "trusted" networks can be authenticated and have assigned rights. On the contrary, networks, which cannot be identified fall outside the boundaries of trust. They are classified as unreliable or as having an unknown security status.

Establishing high quality standards and implementing multiple levels of security are expensive. Therefore, implementation of ICT security measures and the associated additional measures, such as supply chain security and software and hardware QA, should be integrated into the initial project management of nuclear installations, including nuclear power plants, enrichment facilities, radioactive waste facilities and spent fuel storage. This includes ensuring adequate financing budgeted for cyber security at the start of each project.

V. Conclusion

In the future, the demand for better, more modern, more efficient and less obtrusive methods for creating cyber insecurity will grow and contribute to the evolution of cyber weapons. Defending against these risks should be a priority.

While the cyber domain is exceptionally dynamic, cyber governance (technological and legal) is essential for regulating it. This report recommends as essential steps for keeping up with the evolution of cyber security threats the following: information sharing between the stakeholders within the nuclear community; exchange of information in a meaningful and confidential manner; identification of the vulnerabilities and protection of sensitive information; bolstering the communication and cooperation between cyber and physical security; and ensuring that supply chain vulnerabilities are effectively mitigated.

As Carl Sagan noted: *"We live in a society exquisitely dependent on science and technology, in which hardly anyone knows about science and technology."* As Sagan observed the lack of requisite

understanding, I would like to conclude by noting that today's evolving cyber security threat needs to be understood and addressed to ensure a safe future for mankind. Understanding the cyber threat landscape is essential for the proper handling of cyber information threats. Nuclear technologies are the foundation of our future and if we want to continue developing them, we have to manage the risks associated with them. To ensure smooth and secured working processes at nuclear facilities, we must keep pace with the evolution of the cyber security threat.

List of references

1. Alberto Muti, Katherine Tajer and Larry Mcfaul, Vertic report, Cyberspace: an assessment of current threats, real consequences and potential solutions, October 2014, http://remotecontrolproject.org/wp-content/uploads/2014/10/Vertic-Report.pdf.
2. Alena Makhukova, Cybersecurity of Nuclear Infrastructure at the Nuclear Security Summit 2016, CyberPulse #2 (20), June 2016, http://www.pircenter.org/en/articles/2023-cybersecurity-of-nuclear-infrastructure-at-the-nuclear-security-summit-2016.
3. Alexander Klimburg, National Cyber Security Framework Manual, CCDCOE, 2012, https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf.
4. Brent Kesler, Strategic Insights, The Vulnerability of Nuclear Facilities to Cyber Attack, Volume 10, Issue 1, 2011, http://large.stanford.edu/courses/2015/ph241/holloway1/docs/SI-v10-I1_Kesler.pdf.
5. Caroline Baylon, Roger Brunt and David Livingstone, Chatham House report, Cyber Security at Civil Nuclear Facilities: Understanding the Risks, September 2015, https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf.
6. Conference material, Best Practices in Cyber Supply Chain Risk Management, National Institute of Standards and Technology (NIST), http://www.nist.gov/itl/csd/upload/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf.
7. Danny Vinik, America's secret arsenal, 2015, http://www.politico.com/agenda/story/2015/12/defense-department-cyber-offense-strategy-000331.
8. Dustin Volz, U.S. government concludes cyber attack caused Ukraine power outage, Feb 25, 2016, http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K.

9. Dustin Volz, U.S. government concludes cyber attack caused Ukraine power outage, Feb 25, 2016, http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K.
10. James Lewis, Center for strategic and international studies, A note of the laws of war in cyberspace, April 2010, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/100425_Laws%20of%20War%20Applicable%20to%20Cyber%20Conflict.pdf.
11. Javier Solana, BBVA Open Mind, European Foreign Policy and Its Challenges in the Current Context, 2016, https://www.bbvaopenmind.com/wp-content/uploads/2016/01/BBVA-OpenMind-Javier-Solana-European-Foreign-Policy-and-Its-Challenges-in-the-Current-Context.pdf.
12. Liam Nevill and Zoe Hawkins, Special report - Deterrence in cyberspace: Different domain, different rules, July 2016, https://www.aspi.org.au/publications/deterrence-in-cyberspace-different-domain,-different-rules/SR92_deterrence_cyberspace.pdf?platform=hootsuite.
13. Liis Vihul, The Tallin Papers, CCDCOE, The liability of software manufacturers for defective products, 2014, https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_02.pdf.
14. Mary Ellen O'Connell, University of Notre Dam, US, Louise Arimatsu, Chatham House, Cyber Security and the International Law, May 2012, https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/290512summary.pdf.
15. Nuclear industry summit (NIS) 2016, Managing Cyber threat, Working Group 1 Report, March 2016, Washington.
16. Oleg Demidov and Alexandra Kulikova, PIR Center report, Global Internet governance and international security in the field of ICT use, 2015, http://www.pircenter.org/media/content/files/13/14340274400.pdf.
17. Oona Hathaway, Yale Law School, The law of cyber-attack, Jan 2012, http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=4844&context=fss_papers.
18. Pauline C. Reich and Eduardo Gelbstein, Law, Policy and Technology: Cyberterrorism, Information Warfare and Internet Immobilization, p.150_158, 2012, https://books.google.at/books?id=-

76EE2AtQ4AC&lpg=PA158&dq=marco%20gercke%20cyber%20security&pg=PA158#v=onepage&q=marco%20gercke%20cyber%20security&f=false.

19. R.M.Lee, M.J.Assante, T.Conway, German Steel Mill Cyber Attack, Industrial Control Systems SANS, 2014, https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf.
20. Richard Struse, United we stand: Protecting against cyber threats with standards for sharing, The Organization for Economic Co-operation and Development (OECD), Internet Technical Advisory Commitee (ITAC) News, July 2015, https://www.internetac.org/archives/2328.
21. Ryan Singel, White House Cyber Czar: 'There Is No Cyberwar', April 2010, https://www.wired.com/2010/03/schmidt-cyberwar/.
22. Sitara Noor, Cyber (In) Security: A Challenge to Reckon With, 2014.
23. Tim Maurer, The New Norms: Global Cyber-Security Agreements Face Challenges, Feb 2016, http://carnegieendowment.org/2016/02/05/new-norms-global-cyber-security-protocols-face-challenges/iv53.
24. Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control, the International Atomic Energy Agency (IAEA), Technical report series No. 384, 1999, http://www-pub.iaea.org/mtcd/publications/pdf/trs384_scr.pdf.
25. World Economic Forum, PIR Center, Cybersecurity of Civil Nuclear Facilities: Assessing the Threat, Mapping the Path Forward, June, 2016, http://www.pircenter.org/media/content/files/13/14664952850.pdf.