PIR Center, the Centre russe d'etudes politiques within the Workstream on Cybersecurity of Nuclear Installations of the Nuclear Security Global Agenda Council,World Economic Forum

Cybersecurity of Civil Nuclear Facilities:

Assessing the Threat, Mapping the Path Forward

A Policy Memo

Prepared by PIR Center

in collaboration with
the Centre russe d'etudes politiques, Genève

within the Workstream on Cybersecurity of Nuclear Installations
of the Nuclear Security Global Agenda Council,

World Economic Forum

June 2016

Moscow - Geneva

Executive Summary

Cybersecurity challenges have become one of the key concerns for the operators across all critical infrastructure (CI) sectors. Rapid progress in offensive cyber capabilities and upsurge of the number of CI cybersecurity incidents demand urgent reaction from operators, regulators and international community. However, all these stakeholders have to face global trends that obviously increase cybersecurity vulnerabilities of CI objects. Those include extensive and ongoing digitalization of PCS and ICS at critical facilities; broad connectivity of CI corporate office and even industrial networks to the Internet, with the advent of IoT and IoE. Internet connectivity goes hand in hand with "mobile revolution", bringing to CI sectors BYOD an d "CI in your pocket" concepts. Finally, extreme complexity of transcontinental ICS, SCADA software and field devices supply chains has become a common issue for most CI sectors.

Though these trends take place among all CIs, the CNF sector stands out due to a number of its unique characteristics. One of them is unparalleled infrastructural complexity of CNF information systems, measured by hundreds of ICS systems and many thousands of detectors for a single NPP. The factor of extreme complexity generates three pressure points in terms of ensuring CNF cybersecurity. One is unique and one-in-a-kind nature of architecture and engineering cybersecurity and network security solutions at CNF that seriously limit the applicability of previous experience and best practices. Second, trust to vendors and integrity of IT supply chains becomes a grave serious issue. Third, complex environment demands for

a complex and comprehensive cybersecurity approach, including Cybersecurity-by-design (CBD), real-time event management, deployment of cryptography and possibly disclosure of source code of the field devices' firmware by vendors to CNF operators. Second unique characteristic of the CNF sector in terms of cybersecurity is its uncertain place and role of cybersecurity with regard to nuclear security. CNF cybersecurity emerges at the intersection of ICS safety, (physical) nuclear security and information security. So far, the integration of CNF cybersecurity with nuclear security is not over, so it brings a number of challenges, including unclear division of functions among regulators, conflicting requirements, standards and procedures, as well as terminological and conceptual gap between the two security dimensions.

Concerning the regulatory landscape, in most states CNF cybersecurity is just emerging as a separate regulatory framework on a nation-wide level. Key issues include ambiguity in division of regulatory agenda between governmental agencies and gaps and overlaps in the regulators' functions. In many developing countries, these functions are scattered across many regulators with lack of contact between each other. Next issue is lack of a single sector-specific regulator that often leads to weak feedback from private sector stakeholders. Also, the rigid, though highly elaborated nuclear security paradigm sometimes acts as a barrier to elaboration of a hybrid regulatory framework addressing specific issues of the CNF sector. This is often accompanied with the lack of integration of international guidelines, recommendations and best practices into national CNF cybersecurity regulations.

Still, steady progress is observed in many jurisdictions since the beginning of 2010s: elaboration of sector-specific cybersecurity legislation has sped up; increase in regulatory activities focused on CNF cybersecurity takes place even in countries without single sector-specific regulators, e.g. Russia. Finally, the interest of governments in international discussions and initiatives on CNF cybersecurity is growing, judging by their engagement in international conferences and discussion fora.

On the international level, the CNF cybersecurity debate has been taking place in the midst of a legal vacuum and lack of joint incident mitigation and investigation. Thus, no obligatory frameworks are in place to ensure integrity of ICS supply chains for NPPs. Next, cyber-attacks against CNF do not fall under the scope international mechanisms aimed at countering and preventing cybercrime, e.g. the CoE Convention of 2001. Similarly, no ad-hoc international norms or treaties that would address the CNF cybersecurity issue are in place. Proposed treaties and adaptations of existing norms would have limited use and lack compliance incentives unless the issues of attribution and varication in cyberspace are effectively resolved. However, the window of opportunities is open with regard to the UN GGE activities. Proposing the ban of cyber-attacks on CIs and ensuring integrity of IT supply chains in the format of non-binding policy norms might be a major step to advance global CNF cybersecurity debate.

In terms of technical guidelines, trainings, capacity building and awareness raising activities, the IAEA role remains instrumental and is permanently increasing. In 2015, the International Conference on Computer Security in a Nuclear World became a major effort at focusing international attention on the issue. However, to mitigate the threat efficiently, the Agency probably has to push its member states and wider international community towards debate on enhanced and more practical transborder cooperation mechanisms and formats.

Speaking on cyber-threats to CNF, one key thing is that no universally accepted taxonomy of cyber impacts on nuclear facilities currently exists. The IAEA, OSCE and others try to reduce this gap by introducing their classifications, though none of them could be comprehensive. While comprehensive taxonomy is task for the future, a basic reference model with three parameters (source of threat / threat nature / intention) is used to conduct a case-based analysis of 4 cybersecurity incidents at CNF facilities: worm infection of the David-Besse NPP in 2003, Stuxnet and the Olympic Games operation in 2005-2012, cyber-espionage and blackmailing campaign against KHNP NPP operator in December 2014, and worm infection of the Gundremmingen NPP in Germany in April 2016. Analysis of the cases allows to identify some basic trends. First, unlike earlier decades, highly-advanced cyber-threats to CNF tend to prevail today that combine the tools of cyber espionage and cyber sabotage and targeting the critical systems and CNF employees very precisely. Next, revealing and investigating the incident might not be enough to displace the threat once and forever, since the malware has become multi-modular and easily modifiable, while cyber-attacks from short-term spontaneous actions have evolved into continuous well-planned APTs with longstanding lifespans. Finally, threat vectors with regard to CNF cybersecurity incidents drift from traditional spectrum of threats covered by nuclear security. A complex and permanent threat environment has come to the CNF sector, though a bit later then to other CI sectors.

To mitigate these challenges, an integrated system of steps is required on technical, regulatory and global policy-making levels.

Cybersecurity of CNF: Identifying pressure points

In recent years, cybersecurity threats to critical infrastructures (CI) have become a major issue for the operators and regulators. Stuxnet incident, attacks on Thyssen-Krupp steel mill in Germany, energy black-outs in Ukraine and many other incidents demonstrated that offensive cyber capabilities pose real threat that goes beyond disrupting information systems or stealing sensitive information. Critical business processes and operations are physically disrupted, equipment damaged and population exposed to the risk of being cut off from first necessity services and facilities. CIs are targeted across all sectors and industries: energy generation and distribution, transport, oil&gas, aviation, etc. The industries and governments have to respond by adapting their norms, management practices, technical policies and standards, software and hardware to this brand new threat environment. However, they cannot turn the tide of major trends that transform global cybersecurity landscape and, while moving global technological progress forward, also bring new cybersecurity challenges, threat vectors and vulnerabilities to the CI facilities:

- Near-total digitalization of process control systems at CIs. Furnaces, coolant systems, centrifuges, air traffic control lights, power generators and many other critical systems are now operated with the help of digital systems (PLCs, RTUs, software packets like SCADA. etc.) instead of the analog ones. With smart and efficient digital ICS, cyber challenges have paved their way to the process control level, enabling kinetic effects for cyber-attacks that hit field devices.
- Multiple connectivity of CI networks to the Internet. CI corporate networks became connected to the Internet starting from early 2000s. SCADA systems and other industrial software applications are brought online, allowing smarter business process management. Big Data is adapted to ensure more efficient operation of industrial Smart

Grids. Internet of Things (IoT) and Internet of Everything (IoE) are rapidly bringing the industries towards new revolution in process control practices, when each "smart" sensor, actuator or detector installed at the facility is connected online, collects and supplies data online to the enterprise server.

- "Mobile revolution" has reached the CI sector as well. Mobile applications for remote ICS online control appear in the market, implementing the concept "CI in your pocket". BYOD practices have become widely spread across all industries, including CIs, making the situation even more complicated from cybersecurity standpoint.
- Extreme diversity and complexity of supply chains for software and hardware on all levels from office networks servers to PLCs and other field devices. With globalized, transnational and highly competitive IT market, complete vertical integration of IT systems' supply chain has become impossible for any CI vendor or operator. Compatibility and interoperability of systems supplied by different vendors has become a major issue, as well as trust to vendors and ensuring integrity of supply chains.

These trends take place across all CI sectors and industries, and nuclear energy sector is not an exception in this regard. However, because of its specific characteristics, the CNF sector is more "conservative" with regard to some of these trends (Big Data, IoT industrial applications, remote mobile SCADA management, BYOD among the facilities staff). At the same time, the CNF sector has unique characteristics in terms of ensuring its cybersecurity. The way they make cybersecurity issues at CNF differ from any other CI sector is ambivalent. On one hand, civil nuclear facilities almost everywhere are protected with unprecedentedly well-elaborated and comprehensive nuclear security rules and norms that allow to dismiss some cybersecurity issues by default. On the other hand, in some cases the uniqueness of the CNF sector creates pressure points and barriers for effective mitigation of cyber threats.

Some of the pressure points include:

1. Unprecedented infrastructural complexity of CNF IT systems

Though CNF are quite diverse and include quite small research reactors at universities, in most cases, especially including NPPs, they belong to the list of most complex, large-scale and dangerous human-made infrastructures. So NPPs demand extremely complex IT ecosystems to support its operation. To give a better understanding of the issue, it might be helpful to mention that NPPs of last generation with updated IT systems four-layered IT infrastructure, with the corporate network being only the upper one. Each power unit at the NPP is equipped with several dozens of ICS subsystems, all of them need to be properly integrated, secured and made interoperable with the industrial process control software. The total number of IT vendors supplying software and hardware for a single NPP today might exceed 300. Moreover, each power unit today has over 10K of actuators, sensors and detectors sending data to the operators' monitoring systems – and altogether, the IT systems at the NPP today register up to 200K parameter variations per second.

Such complexity has number of implications and pressure points to be addressed.

First, despite the fact that off-the-shelf software and hardware is widely used at CNF, no off-the-shelf solutions for system integration exists in the sector. In terms of its IT infrastructure, each NPP, for example, is a remarkably unique object with original integration solutions. However, in each case the facility's networks and systems also have a unique set of cyber

vulnerabilities and entry points for a potential attacker. This considerably limits the applicability of previous experience and best practices by CNF operators. *Second*, the trust to vendors and integrity of supply chains, especially for ICS becomes a crucial factor. There is simply no way to test thousands of PLCs, RTUs, routers, industrial software applications packets, etc. for hidden functionality, malware, functionality errors, etc. This is challenging since, as said above, each NPP operator has to rely upon many dozens or even hundreds of vendors, most of them transnational companies. *Third*, the complexity of CNF internal cyber environment and intensiveness of data flows demand for a cybersecurity paradigm that would go beyond incident response as such. Several potential elements of such prospective ecosystem could be mentioned:

- Cybersecurity by design for complex CNF objects – a concept that have much in common with the nuclear security-by-design.
- A real-time information security event detection, reaction and traffic monitoring system for all layers of a CNF object, including ICS.
- New rules of the game with suppliers of critical ICS components. Thus, providing the source code of PLCs firmware might be made mandatory for vendor after signing contract with a CNF operator.
- Deployment of cryptographic solutions (digital signatures, protected timestamps) at the lower layers of CNF cyber infrastructure (ICS) in order to strengthen integrity and confidentiality of data.

2. Uncertain place and role of cybersecurity with regard to nuclear security

The CNF security ecosystem includes ICS Safety, combining functional safety of industrial equipment and information security for automated systems. Another element is information security (IS) aimed at ensuring the C.I.A. triad with regard to information processed, stored and transmitted in the facility's information systems (see *Appendix 1*)[*]. This includes both databases in the CNF office network and data received by SCADA software from field devices at the NPP. However, a truly unique for other CI sectors is nuclear security (NS), defined by the IAEA as prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities. Initially nuclear security had nothing in common with cyberspace. However, as new threat vectors emerged, CNF operators, technical specialists and regulators were forced to start integration of the cybersecurity issues into nuclear security paradigm. This process is not over and in some cases that a becomes challenge for ensuring CNF cybersecurity because of:

- Unclear division of functions and resources between the CNF IT\cybersecurity department and divisions responsible for (nuclear) security;
- Conflicting requirements, standards and procedures developed for ensuring nuclear security and cybersecurity;
- Possible restrictions imposed by NS guidelines on major technical upgrades required for ensuring better cybersecurity (deployment of ICS data cryptographic protection).
- Terminological and conceptual gap between cybersecurity and NS staff members, complicating joint mitigation of challenges, prevention of cyber incidents, etc.

[*] Full text of the report, including appendixes, can be found at the web page http://cynuc.pircenter.org

CNF Regulatory landscape: National approaches and international fora

In most countries, CNF cybersecurity is just emerging as a separate regulatory framework on a nation-wide level. Key issues include ambiguity in division of regulatory agenda between governmental agencies and, as a result, gaps and overlaps in the regulators' functions. In many countries, especially developing ones (India, Ukraine, Brazil, South Africa) regulatory functions related to CNF cybersecurity are scattered across several agencies and ministries which often lack proper communication with each other, so issues falling under overlapping authorities are solved in ad-hoc mode. Another issue is lack of a single sector-specific regulator that often leads to weak feedback from other stakeholders: CNF operators and their IT and cybersecurity contractors. That trend may be generalized to the lack of feedback from private sector and expert community, since the stakeholders in some cases are not able to identify proper regulator to address.

Rigid nature of national regulatory frameworks also affects CNF cybersecurity policies, being based either upon well-established nuclear security norms and guidelines, or upon information protection/cybersecurity legislation. Continuity of regulatory paradigm sometimes acts as barrier to elaboration of a hybrid regulatory framework addressing specific issues of the CNF sector. Finally, there is lack of integration of international guidelines, recommendations and best practices into national regulations that are usually restricted to technical guidelines. This refers in first instance to integration of IAEA recommendation and guidelines, and then to documents and recommendations produced by other international fora (World Institute for Nuclear Security (WINS), Nuclear Security Summit). That trend takes place even in advanced states both in terms of nuclear and cybersecurity sector (Russia, USA, France).

However, steady progress on CNF cybersecurity regulation can be observed in a number of jurisdictions since the beginning of 2010s. One of progress indicators that should be mentioned, is that the process of developing and adopting legislation and mandatory guidelines on CNF cybersecurity has remarkably sped up in many states over last 5 years. The list of nations that since 2012 adopted or launched elaboration of sector-specific CNF cybersecurity legislation or detailed guidelines includes Australia, Belgium, Canada, Czech Republic, France, Hungary, the Netherlands, Norway and South Korea with a number of nations to join them in 2016-2017. Many of those nations look to IAEA recommendations and guidelines.

Also, even in states with no single sector-specific CNF cybersecurity regulator and national legislation, increase in regulatory activities focused on CNF cybersecurity takes place, with growing role of CNF operators. One example is Russia where Rosenergoatom Concern OJSC in 2014 started actively adapting broader EOs and requirements on information protection issued previously by the Federal Service for Technical and Export Control (FSTEC) to cybersecurity of NPPs operation. Nations with advanced nuclear energy and cybersecurity sectors regulations actively move from regulating selected CNF issues (protection of information on CNF corporate networks, ICS cybersecurity, proper air-gapping of CNF networks, licensing of CNF IT contractors, etc.) towards comprehensive regulatory frameworks that provide hybrid vision of the issues at the intersection of nuclear security and cybersecurity (for the US and Russian regulatory cases, see *Appendix 2*). The USA should be mentioned here for adopting in 2010 comprehensive and mandatory for all CNF operators NRC RG 5.71 "Cyber Security Programs for Nuclear Facilities".

Finally, growing interest of governments in international discussions and initiatives on CNF cybersecurity is observable. In June 2015, 92 governmental delegations took part in the first International Conference on Computer Security in a Nuclear World at the IAEA's Vienna headquarters, which exceeds the number or nuclear power states. A number of initiatives and proposals coming from nation states have been promoted at international fora. Also, National academia and expert communities have been also demonstrating increasing level of activity in the CNF cybersecurity niche (for details, see *Appendix 3*).

On the international level, the agenda of ensuring CNF cybersecurity and mitigation of relevant cyber-threats to CNF has been developing in the situation of a normative vacuum and lack of joint incident mitigation and investigation. On one hand, this is a standard situation in the field of traditional nuclear security, where threats are usually localized and security and confidentiality considerations prevail over the need in close collaboration. However, this does not work perfectly for the CNF cybersecurity issues since cyber threats are often transborder. Even taking for granted that a certain country ensures perfect protection of its CNF from network attacks, it is still heavily dependent on transnational vendors and supply chains of IT products and services installed at its facilities. E.g., top 3 SCADA software vendors are 2 U.S. and 1 German companies: Schneider Electric, Siemens and Rockwell Automation. For the immense majority of hundreds of hardware and software systems operating at any CNF, most popular solutions are those supplied by large transnational vendors. Total localization of a CNF's IT system is impossible, which makes the operator face the issue of drawbacks, flaws and vulnerabilities in his software and hardware, that can be open the door to various cyber threats. Still, despite this strong case for necessity of international cooperation on CNF cybersecurity, current state of affairs even lags behind cooperation on "traditional" nuclear security issues and mitigation of "analog" threats.

In particular, cyber-attacks against CNF do not fall under the scope international mechanisms aimed at countering and investigation of cybercrimes. The most prominent mechanism is the Budapest Convention on Cybercrime adopted by the Council of Europe in 2001 and open for signing to any nation states. Situation is the same for regional cybersecurity agreements, e.g. the SCO Intergovernmental agreement on cooperation in ensuring international information security from 2009, and bilateral agreements (U.S-Russia set of agreements from 2013; Russia-China agreement from 2015, etc.). CNF cybersecurity incidents also seen to fall out of scope of activities of non-binding transnational collaboration frameworks such as IMPACT-ITU Alliance or FIRST – an international format of CERT-to-CERT collaboration. Furthermore, no international system of standardization has been put in place with regard to specific IT products and services supplied and provided to CNF operators. That might imply requirements to integrity and protection of supply chains of sensitive products (CNF ICS software and hardware components), standards for secure CNF isolation from the Internet, etc. Finally, no common criteria or standards for CNF cybersecurity audit have been developed either.

Similarly, no ad-hoc international norms or treaties that would address the CNF cybersecurity issue are currently in place. Existing international agreements on nuclear security and nuclear nonproliferation emerged before the CNF cybersecurity issue appeared on the agenda; their substantive modification would be a time-consuming effort with no guaranteed result. With regard to global norms, CNF cybersecurity sector just mirrors broader situation with the lack of international regulation of cyberspace as such. However, in recent years several proposals of agreements and norms governing responsible behavior in cyberspace were developed and

promoted at the international fora by Russia and its SCO allies in 2011 and 2015. However, such proposals inevitably lack positive and negative compliance incentives unless the issues of attribution and varication in cyberspace are effectively resolved. That would also be true for any ad-hoc treaty banning attacks on CNF or installations containing dangerous forces (including NPPs), as the latter are defined in Article 56 of the Additional Protocol I to the Geneva Conventions.

At the same time, certain progress and a window of opportunities on the norm-making track appear to take place with regard to the work of the UN GGE on ICT security. In June 2015, the fourth GGE published a report offering the UN member states a set of non-binding volunteer norms framing their responsible behavior in cyberspace. From among such norms, ban of cyber-attacks on CIs and ensuring integrity of IT supply chains can and should be applied to CNF cybersecurity. Although non-obligatory, such norms, if shared and supported by significant number of states, might laid the basis for more advanced legal instruments and serves as a vehicle for strengthened international collaboration with private sector on ensuring integrity of CNF information systems supply chains and other relevant issues.

Meanwhile, at present the crucial role in addressing the CNF cybersecurity issues belongs to IAEA. While the Agency began to raise the topic at its General Conferences starting from 2012, systemic shift towards cybersecurity of nuclear facilities took place in 2013 when the Computer and Information Security Programme was established under the Office of Nuclear Security. The program's goal is to provide member states with the necessary guidance and external expertise to support the detection of and response to intentional cyber-attacks involving or directed at nuclear and other radioactive material, associated facilities and activities. The program encompasses six activities conducted by the IAEA in this area, including: technical guidance documents, technical information exchange forums (CM, TM), regional training activities, regional/international exercise support, subject matter expertise for incident response, and outreach.

Currently, the IAEA recommendations regarding nuclear security refer to cyber security as a factor that may affect the capacity to provide adequate nuclear security and thus should be addressed to sustain nuclear security. In addition, IAEA recommendations issued to support states and operators in the development of nuclear security elements include the notions of the need for protection of computer-based nuclear safety systems and nuclear security systems (physical protection systems and nuclear material accountancy and control systems) against compromise (see *Appendix 4*).

A major initiative launched by the Agency in 2015 was the International Conference on Computer Security in a Nuclear World, which attracted wide international participation. 92 governments and 14 international organizations took part in a five-day conference. 172 reports were made, including some of them providing detailed models of possible CNF cybersecurity incidents resulting from intended multistage cyber-attacks on critical facilities such as NPPs. The Conference format can be a major vehicle of raising awareness of CNF cybersecurity challenges among developing countries and exchange of best practices. Though IAEA technical guidance and recommendations on CNF cybersecurity are not obligatory, they demonstrate increasing relevance for those nation states that are in the initial stages of building regulatory frameworks in this area. Also, in the absence of norms and transborder cooperation mechanisms for CNF cybersecurity prevention, reporting and investigation, IAEA's efforts in the field of raising awareness, capacity building and training gain higher added value. However, to mitigate the threat efficiently, the Agency probably has to push its member states

and wider international community towards debate on enhanced and more practical transborder cooperation mechanisms and formats.

Cyber threats to CNF: Reference model and incident cases

At present, there is no universally accepted taxonomy of cyber impacts on nuclear facilities as well as other CI objects. A three-element classification proposed by IAEA does identify basic types on incidents in terms of their principal consequences. However, it fails to highlight the source and nature of threat, basic technical criteria to describe the incidents such as systems that might be affected, basic possible pathways and scenarios of any purposeful cyber-attack, etc. Some more detailed classifications exist that describe types of CI cybersecurity incidents on the basis of the information system elements that might be targeted. One of such broad classifications for non-nuclear CI was elaborated by OSCE in 2014 (see *Appendix 5*).

With certain exceptions, this approach is also applicable to CNF since the information systems of nuclear and non-nuclear CI still have major similarities. This classification tool might be of use for the IT department of a CNF as a useful theoretical reminder. However, for decision-making process the CNF operator and its cybersecurity department rather needs a multidimensional coordinate axis allowing to classify incident by different criteria, in order to identify whether it comes from human actions, or from technology failures, whether the attacker is insider or an external actor, what the attacker's purpose is and which systems could be affected, etc. This is still the gap to be closed by joint efforts of IT industry, operators and regulators. To make first steps in this direction, a three-criterial reference model could be used to provide some basic structure for cybersecurity incidents at CNF (see *Appendix 6*).

No reliable statistics on cybersecurity incidents exists on the CNF sector since open incident reporting is not the case because of security restrictions and business reputation considerations. Basing on the open data, at least 14 serious cyber security incidents at CNF could be identified over last 25 years (see *Appendix 7*). 13 of them are incidents at NPPs and 1 is the complex Olympic Games campaign conducted against Iran's nuclear infrastructure with the use of Stuxnet, DuQu, Flame and other sophisticated malware. To lay the basis for further research and to accumulate some case-based insights, a study of four cases was conducted (see *Appendix 8*), covering the Davis-Besse incident, the Olympic Games cyber operation, cyber-attack on KHNP, and also infection of the Gundremmingen NPP network in April 2016. The focus was made on intended incidents involving the use of certain malware or other purposeful disruptive cyber tools. Though most of these cases are well known, added value may come from their analysis through the lens of basic reference model and the concept of complex cybersecurity environment highlighted above. However, the KHNP and Gundremmingen NPP cases are quite new and may add new points to the understanding of purposeful cyber-threats to CNF that became a hot topic after the Olympic Games campaign. Summarizing findings of the case-based study, the first thing we would like to point out is the new understanding of the cyber-threat landscape in the area. Further in-depth analysis might and should be helpful here. However, even at this stage, some fundamental trends appear to be evident and demanding concerted reaction from all relevant stakeholders, including CNF operators, IT vendors, national regulators and international fora.

First, unlike 1990s and 2000s, highly-advanced presumably state-sponsored cyber-threats to CNF tend to prevail today, combining the tools of cyber espionage and cyber sabotage and

targeting the critical systems and CNF employees very precisely. *Intended / external / caused by human intervention* incidents emerge as the most serious challenge to CNF cybersecurity. No strategy is in place for effective mitigation of such APT-based challenges, especially on transnational level. This is mostly because of unresolved attribution issues and the absence of international norms and frameworks to address such issues.

Second, revealing and investigating the incident might not be enough to displace the threat. In case of advanced purposeful cyber-attacks targeting CNF, the malware is not a one-shot weapon, like it used to be described. Complex toolkits and multi-module worms have become easily modifiable, each next version presenting a new separate threat to the CI cybersecurity.

Moreover, as the Olympic Games and KHNP cases show, once deployed, the malware often starts to live its own life independently from its authors, becoming an "open-source" malicious project available to all resourceful and skillful actors. A few years after Stuxnet, derivative versions of the Olympic Games arsenal disrupted operations of the Saudi Aramco oil plant industrial network, and infected a number of CI world over, including an NPP in Russia (though not inflicting damage).

Third, threat vectors with regard to CNF cybersecurity incidents drift from traditional spectrum of threats covered by nuclear security. CNF internal security issues meet the Internet security when ex-employees of the South Korean NPP are made a *step 1* target for cyber intrusion. Countering cyber espionage at CNF is also complicated with the necessity to elaborate a counter-strategy to the attacker's media activities. Finally, threats don't come alone anymore – cyberespionage becomes accompanied with "traditional" espionage and cyber sabotage. A complex and permanent threat environment has come to the CNF sector, though a bit later then to other CI sectors. What once used to be short-term occasional incidents, has transformed into advanced campaigns with longer-term lifespans that demand cybersecurity environments with equal lifespans for effective mitigation. Again, this stresses the need for comprehensive real-time cybersecurity strategy rather than "incident response" paradigm.

A Path forward

On *technical level*, new approaches to CNF cybersecurity need to be put in place, primarily through collaboration of CNF operators and IT vendors. The risks of potential hidden functionality in critical IT components (ICS) should be minimized through more intensive and resource-based deployment of penetration testing, fuzz testing, deep scanning of programmable field devices firmware. A major step forward might be a consensus on vendors' responsibility to provide the source code of critical ICS components to contracting CNF operators. The ICS industry would not make such a step eagerly; instead it could be a result of long bargaining between the industry and CNF operators. A balanced and well-thought regulator's move could incentivize ICS vendors to share source codes without forcing them to flee national markets. Cybersecurity-by-design (CBD) might be a major innovation, especially for NPPs and other large CNF. Though its principles are known and share much common with nuclear Security-by-design (SBD), its implementation and technical vision are still under development. More intensive exchange of experience and best practices between leading IT vendors and CNF operators might leverage progress on this issue. Finally, protection from purposeful cyber intrusions into PCS/ICS brings the debate back to integrity and confidentiality of data in CNF critical IT systems. The sector could benefit from deployment of advanced cryptographic tools

in order to ensure better protection of M2M data flows in the ICS. Similarly to the source code issue, this step would not be made easily as it would generate additional costs for CNF operators. However, as recent incidents prove, such costs could be the lesser evil.

On *regulatory level*, deeper integration of CNF cybersecurity into nuclear security approach is a priority aim, allowing to eliminate functional gaps and overlaps between cyber and nuclear regulators. This is also a necessary condition for elaboration of integrated and consistent CBD strategy. At present, this issue has been receiving attention mostly from IAEA. However, this is primarily the issue of domestic policies and internal dialogue between regulators, which should be intensified and promoted by governments domestically. A solid basis for success of such dialogue is comprehensive legislation addressing CNF cybersecurity as a separate issue. For developing states, such legislation is needed just to identify the government's key priorities and to eliminate normative vacuum that prevents CNF operators from developing their internal documents, standards and guidelines. For promotion of such domestic activities, IAEA and other international fora are still instrumental, since they accumulate best practices from advanced member states and could provide blueprints and reference models for the developing ones. Marrying the worlds of CNF cybersecurity and nuclear security also requires extensive work with human capital. Governments and CNF operators have to breed a generation of specialists with a new mindset and vision of the issue, a different one from traditional nuclear security approach but able to complement and enhance it. Domestically, it could be supported through innovations in the higher education system and support of trainings, workshops and dialogues involving both nuclear and IT industries. The work of think tanks and NGOs on training and awareness raising on these issues should be supported. Internationally, the IAEA trainings, exercises, awareness raising and capacity building activities remain crucial.

On *international norm- and policy-making* level, smooth progress is hardly expected. Mandatory intergovernmental agreements on mitigation of cyber-threats to CI are not on the horizon, while the debates on adaptation of existing international law to cyber challenges could take decades and result in no practical cooperation mechanisms. Also, existing transnational anti-cybercrime mechanisms could hardly encompass CNF sector because of national security restrictions. The debate within all these fora makes sense and should go on, though it would hardly deliver fruits in a short-term perspective. Still, certain opportunities are open with the UN GGE format. In Summer 2016, the fifth session of the Group starts its meetings, and that might be a chance to agree and propose volunteer norms of responsible behavior that would address some sector-specific CI. The decision on which CI sector should be addressed first has not been made so far, and this is the opportunity to bring CNF cybersecurity to the forefront of the Group's agenda. So the next GGE report might include a volunteer norm banning state-sponsored attacks on CNF or suggesting some mechanism of self-restriction with regard to such actions. Even if non-binding and lacking compliance, such norm would help to promote the debate on CNF cybersecurity and approximate some future mandatory intergovernmental mechanism. Also, the Group could be instrumental for resolving the terminology and classification issue with regard to CI sectors and taxonomy of cyber-attacks against them. That would be a brick in the wall of common language and shared visions of CNF cybersecurity on the international level. Finally, some of earlier GGE proposals could be updated to address particularly the CNF sector, including the norm on ensuring the integrity of supply chains for critical IT systems. Apart from UN GGE, international PPPs such as IMPACT-ITU could be helpful for exchange of data on CNF cybersecurity incidents, accumulation of best practices and creation of databases of vulnerabilities, malware and hidden functionalities used in cyber-attacks against CNF.

List of abbreviations:

APT – Advanced persistent threat
BYOD – Bring your own device
CBD – Cybersecurity-by-design
CERT – Cyber Emergency Response Team
CI – Critical infrastructure
C.I.A.– Confidentiality – Integrity – Availability *(classic information security triad*)
CNF – Civil nuclear facility
IAEA – International Atomic Energy Agency
ICS – Industrial control system
IS – Information security
IT – Information technology
IMPACT-ITU – International Multilateral Partnership Against Cyber Threats – International Telecommunication Union Alliance
NPP – Nuclear power plant
NS – Nuclear security
OSCE – Organization for Security and Co-operation in Europe
PCS – Process control system
PLC – Programmable logic controller
PPP – Public-private partnership
RTU – Remote terminal unit
SBD – Security-by-design
SCADA – Supervisory Control and Data Acquisition
SCO – Shanghai Cooperation Organization
UN GGE – United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security