PROTECTING NUCLEAR INFRASTRUCTURE: THE NEED FOR COORDINATED ACTION IN THE DOMAIN OF TECHNICAL STANDARDIZATION, COORDINATED STRATEGY AND EXCHANGE OF INFORMATION

Oleg Demidov, PIR Center[1]

Evolution of Threats: Ever Going On

At first glance, last couple of years added nothing new to the global cybersecurity threat landscape of the nuclear energy industry and its incident track records. The last major publicly reported cybersecurity incidents were cyber-attack on KHNP in late 2014-early 2015, and worm infection of the Gundremmingen NPP network in April 2016.

However, one hardly may say that since those incidents the cyber threat to civil nuclear facilities has not advanced or evolved. However special, the infrastructure of the nuclear energy industry has much in common with other energy sectors – particularly including ICS systems, its security policies and general weak spots might take advantage of. So a number of cases took place since 2015 proving that ICS across all sectors continue to face mounting threat of purposeful targeted cyber attacks. The Ukrainian case with cyber operation against power grid operated by Prykarpattyaoblenergo in December 2015 has become a prominent case of compromising ICS cyber security and triggering wide-scale disruption of a vital public facility.

Although the attack on Ukrainian power grid has been attributed to a government-affiliated advanced persistent threat (APT) by many Ukrainian and Western experts, serious cyber threats to ICS of critical infrastructures nowadays do not even need to be precisely and uniquely targeted. Moreover, they do not even need to target specific ICS components to be able to disrupt industrial or other technological process. The best proof are recent widespread attacks by ransomware – malware encrypting information on hard drives of systems run by specific OSes. Just a few years ago, ransomware was regarded as a nasty, but not particularly dangerous tool for small criminals attacking n encrypting personal devices. **The notion of ransomware was quite far from the domain of industrial equipment and critical infrastructure security. That changed rapidly with recent global ransomware attacks.**

The brightest example is WannaCry global ransomware attack, that took advantage of the EternalBlue exploit based upon SMB-1 protocol vulnerability in Windows-operated systems that was originally discovered by the U.S. National Security Agency. Of course, WannaCry did not affect any nuclear energy facilities – but it did disrupt technological processes and operation of equipment in other sectors. Thus, up to 70,000 devices, including computers, MRI scanners and blood-storage refrigerators may have been affected in National Health Service hospitals in England and Scotland. Auto manufacturers, including Nissan Motor Manufacturing UK and Renault, had to halt some of their assembly lines when trying to stop dissemination of the ransomware

[1] The materials, judgments and conclusions contained within the article represent solely the views of the author. No reproduction or quotation is permitted without reference to this of article.

across their systems. The total economic damage caused by WannaCry campaign is estimated to be around $1 bln. The key thing is that it could be much worse if the exploit and other malicious code of the ransomware had been specifically targeted to hit Windows-run SCADA systems at critical infrastructure objects. Those are also installed at NPPs and other nuclear energy facilities.

And, of course, there is no way for May 2017 wave of WannaCry to be the last massive ransomware attack. Just in the week of June 19 Honda Motor Co. had to halt production at its Sayama vehicle plant near Tokyo after finding out that WannaCry hit its networks massively.

Finally, **brand-new threat vectors and malware concepts targeting ICS and industrial equipment also emerge.** In May 2016, a group of German researchers presented a proof-of-concept of a first ever computer worm able to spread itself infecting directly programmable logic controllers (PLCs), model Siemens SIMATIC S7-1200v3 and the industrial protocol S7. The thing is the malware does not need to infect any industrial computer or server before hitting the ICS equipment – its whole operation and self-dissemination lifecycle takes place directly on the level of PLCs. One should not let his guard down because of the fact that the worm's (PLC-Blaster) proof-of-concept was made and presented not by a malicious APT, but by security researchers team. What once is invented as a warning from researchers, could be with ease reinvented and used for malicious purposes by other actors.

So far, **all these threats and malware tools hit targets somewhere next to nuclear energy infrastructures.** Certainly, this could not be regarded as a luck or occasion, since security regime, air-gapping, network segmentation and infrastructural peculiarities protect nuclear installations from sporadic threats without precise targeting, such as WannaCry and the like. However, all those cases just show that cyberthreat environment for critical infrastructures, including nuclear facilities has become more aggressive and dense than ever before.

The need for action: stressing the role of technical standardization

One of major areas where international cooperation is needed as well as exchange of experience and best practices between leading countries and the developing ones, including nuclear energy newcomer states, is **technical standardization.**

A notable recent achievement on the level of global standardization was elaboration and adoption of IEC 62645:2014 "Nuclear power plants - Instrumentation and control systems - Requirements for security programmes for computer-based systems" – a 2014 global standard by International Electrotechnical Commission. The standard establishes requirements and provides guidance for the development and management of effective security programmes for Instrumentation& Control (I&C) computer-based systems for nuclear power plants (NPPs). What is also important, IEC 62645:2014 describes path towards integration of Hardware Description Language Programmed Devices (HPL/HPD) in the I&C systems of NPPs. The major goal of the standard was to define appropriate programmatic measures for the prevention of, detection of and reaction to

malicious acts by digital means on I&C systems of nuclear objects – including purposeful cyber attacks in first instance.

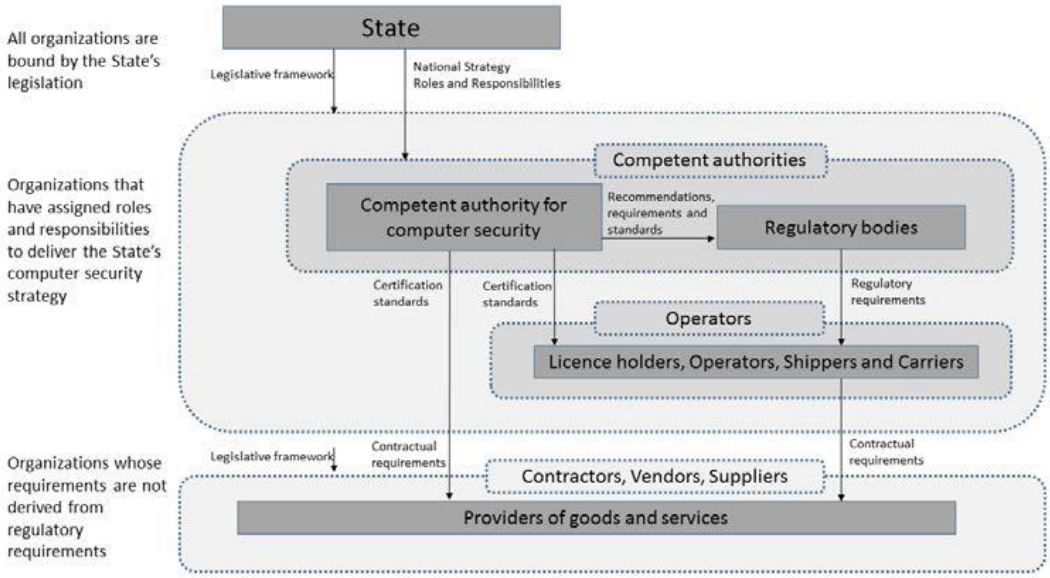
Also, IEC (ISA) 62443 family of standards ("Security for industrial automation and control systems") has been developing as well. Originally, the standards in this series were developed by the International Society for Automation (ISA) and released as American National Standards Institute (ANSI) documents. Later, in 2010, they were renumbered to be the ANSI/ISA-62443 series and eventually integrated in the system of the IEC standards. So now, this series has become a golden standard for industrial automation deployment, industrial network segmentation and ensuring security in a specific environment composed of industrial hardware and industrial protocols. In 2016, another development of the series was drafted – ISA-62443-4-1 "Product Development Requirements". The draft new standard aims to define the development process that should be used to create products that make up the industrial automation and control system. This direction of standardization is particularly important for ensuring future cybersecurity at nuclear energy installations. One of major problems of today's solutions for ICS, including those deployed in nuclear energy sector, is that they miss security on the level of design and basic architecture, such as key protocols for exchange of data in industrial networks. One of potential ways to change it is to elaborate next generation of ICS for critical infrastructures basing upon the concept of cybersecurity-by-design.

Another important step has been initiated by IAEA. In December 2016, the Agency finalized elaboration of a draft of its new publication from Nuclear Security Series - NST045 "Computer Security for Nuclear Security. Draft Implementing Guide". Although IAEA publications are neither standards nor binding recommendations, they still matter for laying the basis for widely shared, common approaches towards ensuring cybersecurity at nuclear facilities.

One of the most important and valuable things about NST045 is that the draft publication provides integrated scheme depicting computer-related functions and responsibilities of different actors with regards to nuclear security regime. Principal added value of this scheme and the approach embedded in it is its comprehensive, multilevel and cross-structural nature. This is something that was missing in previous IAEA publications and probably in the Agency's approach as such. Certain level of maturity of the expert understanding and the Agency's practice was necessary to jump from separate computer security issues to a nearly holistic framework for the nuclear industry. Even more value this integrated approach has for regulators in developing countries with national nuclear energy sector. All of them are solving the puzzle of building national regulatory ecosystem for nuclear security, including its computer aspects. So providing them with a blueprint framework of such ecosystem might be of much use.

The only level which unfortunately is missing in this scheme is transnational – it is also necessary since all national operators of nuclear energy facilities are dependent upon global ICS vendors, and all of them have reasons to maintain protection against transborder, transnational cyber threats to their facilities. So it would make sense to add

international level to this framework – probably including IAEA itself – not as a regulator, but as a potential coordinator of joint efforts and facilitator of exchange of best practices, experience, training and capacity building activities, etc.



Source: *FIG. 5 Organizations with computer security responsibilities in a nuclear security regime. COMPUTER SECURITY FOR NUCLEAR SECURITY DRAFT IMPLEMENTING GUIDE. IAEA, NST045 DRAFT, December 2016.* http://www-ns.iaea.org/downloads/security/security-series-drafts/implem-guides/nst045.pdf.

However, any steps forward made on the level of international standardization still needs to be implemented in national standards and practices of NPPs' operators. Adaption of global technical standards to national standardization system and their implementation into daily business processes takes a lot of time, institutionalized will and resources. For many countries, this quest might take many years or even several decades to complete.

The more important is the progress that certain nuclear energy powers achieve in recent years when it comes to building an integrated regulatory framework for nuclear cybersecurity from a set of scattered acts and practices. One of examples of such progress demonstrates Russia.

Russia: Increasing Efforts in Standardization and Policy-Making

In recent years, Russia has demonstrated considerable progress with elaboration of comprehensive approach towards standardization and building institutional capacities for ensuring of cybersecurity at NPPs and other civil nuclear installations.

In Spring 2017, a new technical committee (TC) No. 194 "Cyber-Physical Systems" was established in the structure of Russian national standardization body – Rosstandart. According to the plans announced by its Secretariat, the TC together with the industry shall conduct work on developing next generation standards for CPS in major niches

and sectors. Some part of this work might involve ICS segment and cover security aspects of their functioning.

Previously, in 2016 the Russian VNIIAES (All-Russian Research Institute for NPP Operation), a subsidiary of Rosatom State Corporation, announced the program to ensure protection of ICS of all Russian NPPs from cybersecurity risks. First phase of the program implies elaboration of a new concept for ensuring cybersecurity for ICS at NPPs[2]. Next step includes comprehensive assessment and review of protection against cyber threats currently provided for ICS at Russian NPPs. Finally, basing upon the results and findings of the previous steps, new software and hardware systems would be installed in order to ensure complex protection of ICS at Russian nuclear power plants against full spectrum of cybersecurity risks and threats. This major effort is expected to be implemented in collaboration with a new body created in the structure of Rosatom – RASU (Rosatom ICS) as recently as in February 2016. Establishment of a separate entity working on ICS for NPPs and other installations operated by Rosatoms illustrates increasing importance of ICS and computer security for Russian nuclear energy industry.

Also, in late 2016, VNIIAES announced that it started elaboration of a new standard "Instrumentation&Control Systems. Cybersecurity of ICS of NPPs. Terms and definitions". The standard is supposed to take into account best practices, approaches and recommendations provided in recent IAEA publications and IEC standards (such as aforementioned IEC 62645:2014 and IEC 60880:2006 "NPPs – I&C systems important to safety – Software aspects for computer-based systems performing category A functions" – and others). However, the basis of the standard is supposed to summarize and describe an original Russian approach to ensuing cyber security of NPPs. The ICT technical standardization track in Russia recently has entered the phase of new developments in connection with the course towards building the national "digital economy" and achieving "digital transformation" of the national industry. This process also might involve ICS and cyber physical systems, including those designed for and deployed at civil nuclear facilities.

Standardization and practical efforts in nuclear cybersecurity area in Russia follow in parallel with legislative developments. In December 2016, the draft Federal Law on Security of Critical Information Infrastructure (CII) of the Russian Federation was submitted to the Russian parliament. The draft law provides systemic methodology for categorization and identification of CII objects in all major sectors – nuclear energy sector is expressively listed among them. Not only the proposed legislation sets the basis for terminology (including ICS, computer incidents and computer attacks), but also it introduces a consistent system of cybersecurity obligations and requirements to operators of CII objects, gives federal legal ground to the all-nation State system for prevention, detection, and mitigation of consequence of computer attacks (GosSOPKA). All these measures cover nuclear energy sector, so these developments

[2] ВНИИАЭС проведет анализ состояния защиты АСУ ТП всех действующих АЭС от киберугроз http://www.rosatom.ru/journalist/news/vniiaes-provedet-analiz-sostoyaniya-zashchity-asu-tp-vsekh-deystvuyushchikh-aes-ot-kiberugroz (last accessed June 21, 2017)

would strengthen cybersecurity and resiliency of Russian nuclear energy industry – and also generate valuable experience that should be promoted internationally and shared with "nuclear energy newcomers" and developing states. Once again, the IAEA could play the role of aggregator of such experience and a venue for its sharing.

Instead of conclusion: Global agenda for information sharing and incident response

- **Standards and normative regulations are necessary, but not enough tools to combat cyber threats to civil nuclear facilities on the global level.** Technical standardization and building of comprehensive regulatory frameworks on the national level are the essential basis for ensuring cyber security in the nuclear energy industry. However, on top of that basis further constructions need to be erected, and they need to ensure transnational scope of coordinated action.

- **One of the potential vehicles for such coordinated actions could be the process of implementations of trust and confidence building measures developed within certain international formats**, including OSCE. On March 10, 2016 the Permanent Council of OSCE adopted Decision No.1202 "Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies".[3] The document expands the initial set of cyber-TSBMs outlined by OSCE in December 2013, and focuses predominantly on critical infrastructure (CI) protection. Article 15 of Decision No. 1202 encourages states to facilitate regional collaboration between legally-authorized authorities responsible for securing CIs to discuss opportunities and address challenges to national as well as trans-border ICT networks, upon which such CI relies. This includes developing shared responses to computer incidents affecting CIs and sharing information on cyber threats to CIs on the regional and subregional level. Also importantly, Article 16 suggests that states encourage reporting of vulnerabilities affecting the security of CIs and share associated information on available remedies to such vulnerabilities, including with industry and private sector.

  Since nuclear energy industry does belong to CIs in any of existing classification, these mechanisms could be of much use for advancing regional collaboration among nuclear facilities operators and regulators in the European region. Of course, the key obstacle is severe lack of trust that would be hard to overcome. However, one possible step in this direction might be shifting the momentum of such collaboration to private sector and PPPs. Shared approaches might be built upon shared solutions and mechanisms. Thus, in 2016 Russian Kaspersky Lab announce its initiative of a CII-CERT designed to provide

[3] Decision No. 1202.OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from The Use of Information and Communication Technologies
http://www.osce.org/pc/227281?download=true (last accessed June 21, 2017)

services both for government agencies – and private entities, including nuclear energy industry actors. Although this initiative at the first stage targets Russian customers, nothing prevents it from going regional in the future – probably, except toxic fallout from mass accusations of 'Russian hackers".

- **Finally, IAEA itself is the key structure and authority that could design and engineer the perspective mechanism of international collaboration against cyber threats to nuclear energy industry.** The first thing that comes to mind is creating under IAEA the global repository of malware and vulnerabilities that were or potentially could be used in cyber-attacks against peaceful nuclear installations. Due to grave trust issues, the information in such repository could be available to a restricted number of subjects, including NPP operators and certain major vendors of critical ICS components for nuclear industry operators. IAEA with its reputation would guarantee protection of such sensitive information on vulnerabilities and restricted access to it. Finally, in the horizon of 2020 the Agency could expand the format and functions of its Incident and Emergency Centre (IEC). It becomes more and more obvious that **cyber incident management profile should be added to the IEC functions**, so that the Centre could become a focal point for national and industry CERTs, and security operation centers (SOC) of nuclear industry operators. Also, the IEC could provide consultations, information and other assistance to nuclear energy newcomer states trying to secure their objects against cyber threats. Finally, in a more distant perspective the IEC could really take certain functions of a CERT, providing technical consultations to operators in cases of cyber incidents or their immediate threat.

  No technical or financial obstacles make these ideas impossible – it is just a matter of trust and political will that should be generated and promoted in all frameworks, including the UN among the key ones.