Cybersecurity of Civil Nuclear Facilities:

Assessing the Threat, Mapping the Path Forward

Appendices

to the 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,

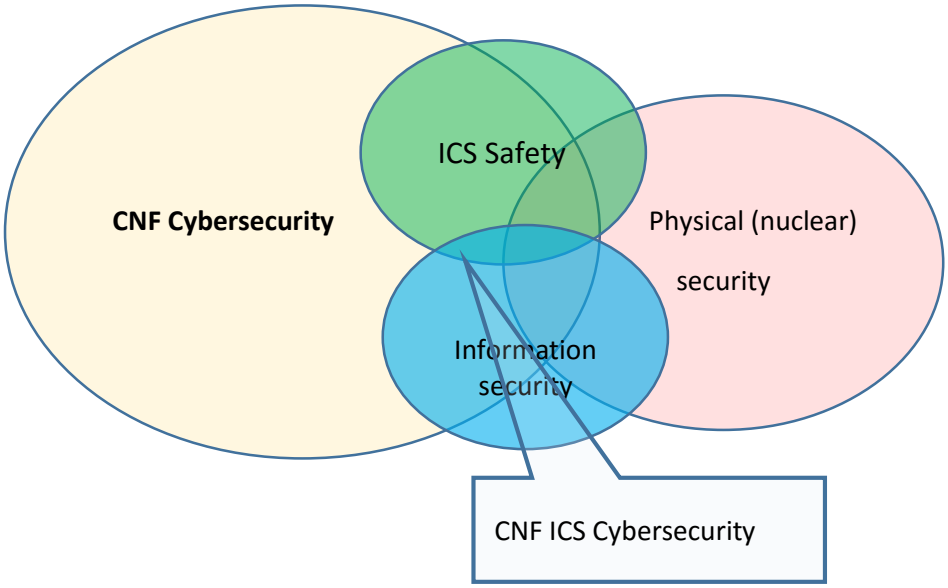
World Economic Forum

June 2016

Moscow - Geneva

List of Appendices:

Appendix 1. <u>CNF sector basic security ecosystem</u>



Appendix 2. Regulatory approaches towards CNF cybersecurity: USA and Russia cases

A) Russia

In Russia, the Federal Service for Technical and Export Control (FSTEC) historically has been in charge of information protection. The service issued requirements for state secrets and confidential data processed in information and automated systems. First sets of such non-classified requirements issued from 1992 did not pay and specific attention to protection of information related to CNF. Confidentiality was regarded a top priority among the C.I.A. triad. The change took place gradually in 2000s when the nuclear industry corporations, including Rosatom and its subsidiaries started to adapt FSTEC requirements as a basis for their internal documents. In 2006, the Model Guidelines for protection of information in automated systems of business entities and organizations were adopted. In 2011, Rosenergoatom Concern OJSC adopted the executive order "On measures to prevent uncontrolled access to hardware and software tools of ICS.

Next wave of regulatory activities was launched by FSTEC in 2012, when the need in revision of existing documents and their update with regard to recent developments on the IT area became obvious. At first, these revisions did not address CNF directly. However, in 2014 the Executive Order No. 31 "On information protection in ICS of critical objects and high technical hazard infrastructures" was adopted that also addressed CNF among other CI. A major conceptual change took place, since the focus in the new document shifted from confidentiality to availability and integrity of information, and continuity of critical business processes. However, major drawback of the EO was the lack of its connection to any federal law, which questioned its mandatory status for CNF and other CI operators. The issue was complicated by the fact that draft law "On CII security" elaborated by FSB in 2013, has not been adopted so far; thus, the legal basis for such EOs is still missing on the level of federal legislation.

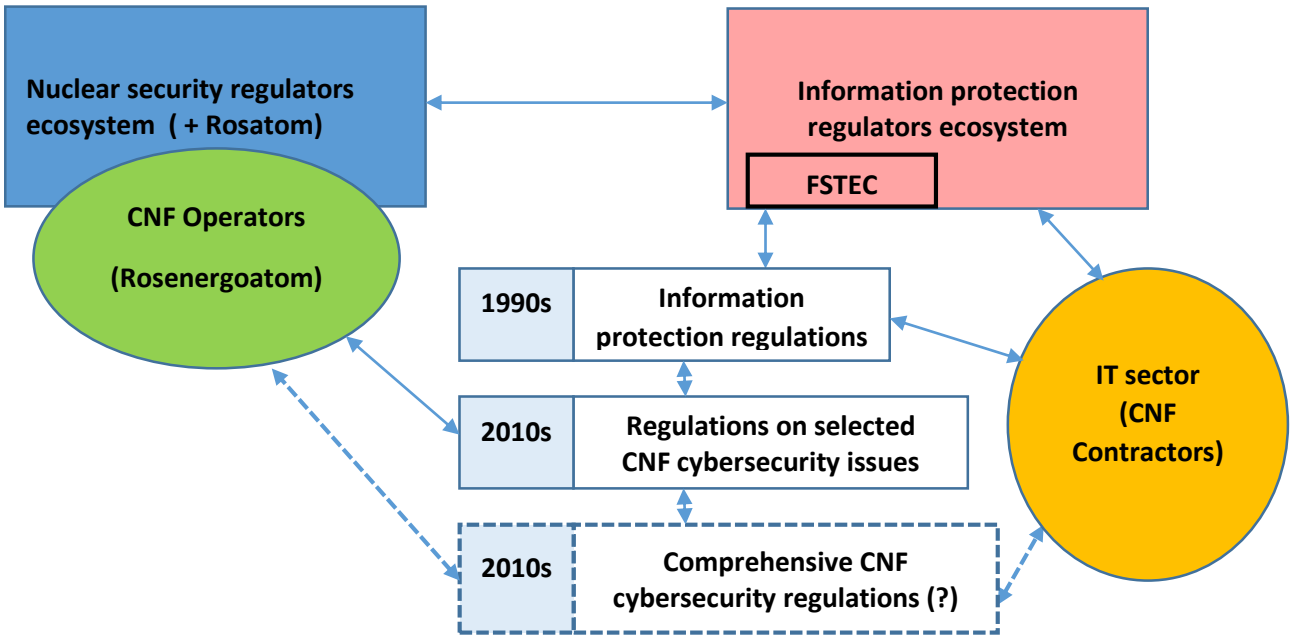
In these circumstances, the compensation of higher-level regulatory vacuum has become the task of CNF operators. In 2014, Rosenergoatom issued mandatory "General provisions on ensuring information security of ICS at NPPs", loosely based on FSTEC regulations from 2012, which resulted in a strong accent on ensuring protection of information in corporate databases instead of securing the ICS operation cycle from cyber threats. Still, the document sets general principles and provides a basic framework for further elaboration of detailed technical and organizational measures to ensure information security and cybersecurity at NPPs. This work was already started by Rosenergoatom in 2015. Also, two more documents dedicated specifically to protection of information in ICS of NPP's have been elaborated by the Concern starting from 2015.

Summarizing the evolution of CNF cybersecurity regulations in Russia, two points should be stressed:

- At present, major efforts in this field have been made by CNF operators themselves, including Rosenergoatom, since no federal law on CII has been adopted and FSTEC regulations are not comprehensive enough with regard to specific CNF cybersecurity niche.

- Almost all existing regulatory documents are based on Russian information protection approach and conceptual framework, which brings two implications. On one hand, the regulatory documents address technical side of the issue in a very thorough and detailed manner. On the other hand, they lack focus on wider aspects (cybersecurity culture in nuclear energy sector, capacity building, awareness raising, international cooperation) and do not incorporate and reflect IAEA guidelines and recommendations.

Russia CNF cybersecurity regulations: progress scheme



B) USA

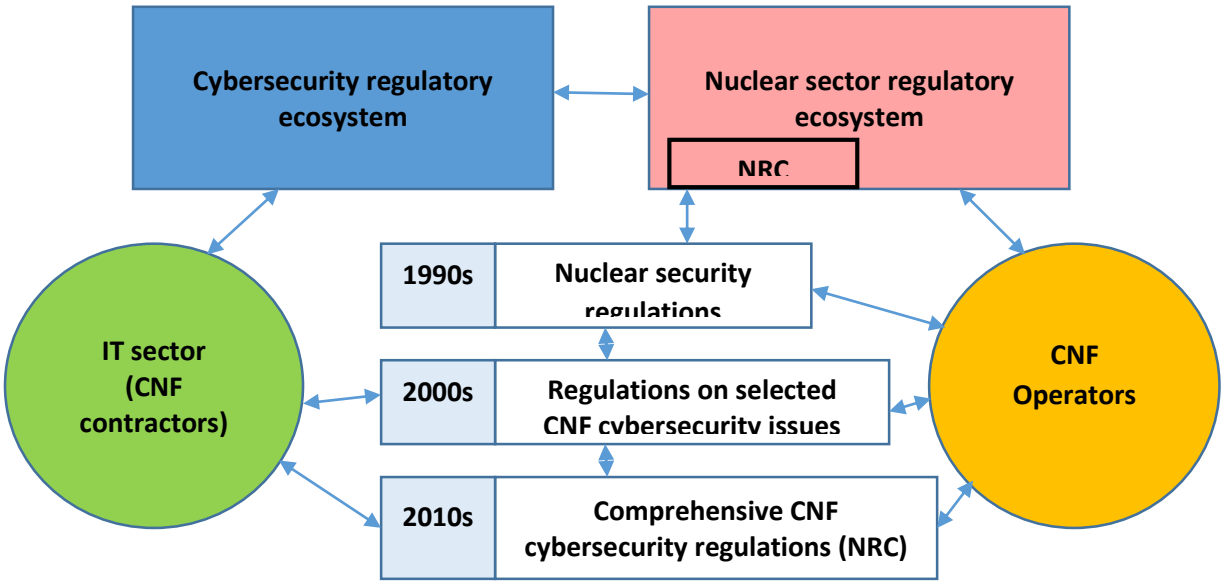
The U.S. key regulator in charge of civil CNF protection is Nuclear Regulatory Commission (NRC). In past decades, NRC documents were reasonably focused on traditional nuclear security issues and challenges (Regulatory Guide 5.66 "Personnel Access Authorization for NPPs", Regulatory Guide 5.77 "Insider Mitigation Program", etc.). The issues of CNF cybersecurity started to be addressed by the regulator in early 2000s. The first regulatory move took place in 2002: NRC Order EA-02-026 "Interim Safeguards and Security Compensatory Measures for NPPs" established the requirement for mandatory licensing for contractors ensuring cybersecurity at NPPs. Identical requirements were adopted by different regulators with regard to other U.S. CIs.

In 2004, the issue of self-assessment of NPP operators in the field of cybersecurity was addressed in the NRC's document NUREG/CR-6847. This move coincided with the work conducted by the U.S. Nuclear Energy Institute (NEI): in the 2005, it published "Cyber Security Program for Power Reactors" guidelines addressed to U.S. NPP operators. Despite two documents and institutions made focus on the same issues, the NEI guidelines were not agreed upon with NRC. The Institute continued to work on its guidelines and documents independently

from the operator, further addressing CNF cybersecurity issues in a document of broader scope - “Cyber Security Plan for Nuclear Power Reactors”.

However, NEI activities incentivized the Commission to address CNF cybersecurity issues in a more detailed and comprehensive way. In 2007 and 2009 a series of two NRC documents followed that were focused on protection of software, computers and networks at CNF (“Guidance on Software Reviews for Digital Computer Based Instrumentation and Control Systems”, NRC BTP 7-14 and “Protection of Digital Computer and Communication Systems And Networks”, 10 CFR 73.54). Finally, the comprehensive approach to regulation of CNF cybersecurity was put in place in 2010 when NRC elaborated, proposed for discussion and then adopted the document RG 5.71 “Cyber Security Programs for Nuclear Facilities”. The document was based upon particular Special Publications (SPs) developed by National Institute of Standards and Technology (NIST) and providing comprehensive set of protection measures for state information systems. Adapting these measures to nuclear energy sector and collecting feedback from the CNF operators, NRC managed to elaborate mandatory, comprehensive and systemic regulatory document for all U.S. nuclear energy sector operators and contractors. NRC RG 5.71 includes 147 protection measures, including 71 technical, 67 operational and 9 administrative ones.

USA CNF cybersecurity regulations: progress scheme



Comment to schemes above: In general, U.S. regulatory track record in the CNF sector demonstrates certain similarities with the Russian approach:

- Mandatory licensing for all contractors providing information protection services to CNF was introduced quite early.
- The regulatory approach with regard to the CNF sector evolved in a similar way: relevant regulators developed their documents basing them upon broader norms adopted previously for information protection of critical objects or governmental information systems in general.

Although in both countries current level of CNF cybersecurity is quite advanced, the regulatory documents pay relatively few attention to certain non-technical issues promoted by IAEA (trainings, awareness raising, capacity building) and do not regard international cooperation as a priority goal. However, Russian regulatory documents are more rigid in that regard.

Appendix 3. Governmental and academia initiatives on CNF cybersecurity

Governmental initiatives:

- At the 2012 Nuclear Security Summit (NSS) in Seoul, the UK sponsored a Multinational Statement on Information Security, which attracted 31 signatures (and 4 more lately).
- UK and the Netherlands have supported the WINS and IAEA initiatives on CNF cybersecurity. The two states also took leadership role in promoting the CNF cybersecurity agenda at the NSS in 2014 in The Hague.
- In 2012, Denmark organized international table-top exercise on CNF cybersecurity *@tomic-2012* conducted with the participation from the IAEA, the European Commission, INTERPOL and the UN Interregional Crime and Justice Research Institute.

Non-governmental and academia initiatives:

- In 2013, the Kings College London in partnership with the UK Foreign and Commonwealth Office have drafted a Code of Conduct on Nuclear Information Security providing basic guidance for CNF operators and individuals on strengthening nuclear information security culture.
- In 2013, the Russian PIR Center conducted a workshop with participation of Russian CNF operators and the Dutch MFA and proposed to adopt international soft law regulations to strengthen CNF cybersecurity.
- In-depth research projects on CNF cybersecurity were launched in 2014-2015 by the U.S. East-West Institute, NTI and the UK Chatham House, the Royal Institute of International Affairs.

Appendix 4. IAEA Technical guidelines and recommendations on CNF cybersecurity

IAEA technical recommendations containing notions of the need for protection of computer-based nuclear safety systems and nuclear security systems:

- IAEA Nuclear Security Series Publications No. 20 “Objective and Essential Elements of a State’s Nuclear Security Regime”
- IAEA Nuclear Security Series Publications No. 13 “Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities” (IAEA INFCIRC/225 Rev.5).

IAEA technical recommendations on protection of computer-based systems at nuclear facilities:

- IAEA Nuclear Security Series publication No. 17 “Computer Security at Nuclear Facilities” published in 2011 as one of its technical guidelines series on nuclear security.
- IAEA Nuclear Security Series publication No. 23-G “Security of Nuclear Information” published in February 2015 and focusing on privacy and other aspects of information security (integrity and accessibility) in the area of nuclear security. This document essentially bridged the gap between the existing state and industrial requirements on cybersecurity and their applicability in nuclear energy industry.

Appendix 5. OSCE Classification for cybersecurity incidents at non-nuclear CI objects

Source: Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace. Organization for Security and Co-operation in Europe, 2014.

- Unauthorized use of remote maintenance access points;
- Online attacks via office or enterprise networks;
- Attacks on standard components used in the ICS network;
- DDoS attacks on Internet-connected segments of corporate network;
- Human error and sabotage;
- Introducing malware via removable media and external hardware;
- Reading and writing news in the ICS network;
- Unauthorized access to resources;
- Attacks on network components;
- Technical malfunctions or force majeure.

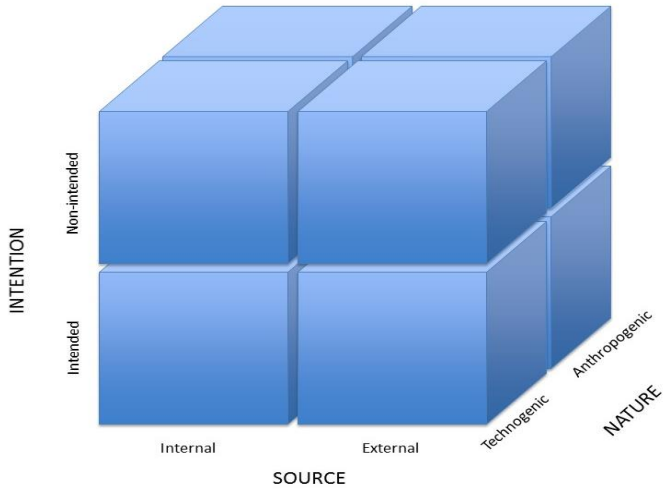
Appendix 6. <u>Basic reference model for CNS cybersecurity incidents</u>

- Source of the threat:
  - Internal source (malicious insider, hardware or software failure, etc.).
  - External source (external attacker, impact of software and hardware failures of external infrastructures and systems on the CNF networks and IT equipment, etc.).

- Threat nature:
  - Technical (industrial equipment, software or hardware incurred impact without direct human intervention)
  - Human factor (incident caused directly by human intervention into the CNF operation, regardless of insider's or external position of the actor)

- Intention:
  - Intended incident (network attack on a CNF corporate network, purposeful disruption of the facility's ICS, insider's purposeful manipulations with data flows and digital controls, etc.).
  - Non-intended incident (SCADA operator's mistake, using an infected USB-stick on the CNF industrial network unknowingly, etc.).

CNF cybersecurity incidents basic reference model visualization:



Appendix 7. Reported cybersecurity incidents at CNF since 1990

Incidents	**Classification**
Japan, 2005	Intended/ internal / technical
Ignalina NPP USSR 1992 Bradwell NPP, UK, 1999	Intended / internal / human factor
Monju NPP, Japan, January 2014 Areva, France, September 2011	Intended / external / technical
Stuxnet, 2010 KHNP, South Korea, December 2014	Intended / external / human factor
Sellafield NPP, UK, 1991 San Onofre, US, 2012 Susquehanna, US, 2012 Browns Ferry NPP, US August 2006	Non-intended / internal / technical
Hatch NPP, US, March 2008; Miami, US, 2008	Non-intended / internal / human factor
Davis-Besse NPP, US, 2003 Gundremmingen NPP, Germany, 2016	Non-intended / external / technical

Appendix 8. Selected CNF cybersecurity incidents: a case-based analysis

Case 1: Davis-Besse NPP incident, 2003

CNF affected: Davis-Besse NPP with single pressurized water reactor, location: Oak Harbor in Ottawa County, Ohio, USA.
Incident classification: Non-intended / external / technical.
Malware used: SQL Slammer computer worm.

On January 25, 2003 at 05:30 UTC SQL Slammer, a primitive computer worm, started to infect hosts on the Internet. The worm exploited a buffer overflow vulnerability in Microsoft SQL servers and Desktop Engine database products. The vulnerability did not belong to the zero-day class: a patch for it had been released by Microsoft six months prior to the incident in MS02-039 package. However, hosts that were still running unpatched copies of Microsoft SQL Server Resolution Service listening on UDP port 1434, were vulnerable, so many of them become infected with Slammer. After infection, the hosts were used to create new copies of the worm and disseminate them to randomly scanned addresses on the Internet. Since many servers remained unpatched for this particular vulnerability, 75 000 got infected in a few minutes. Spreading so fast, Slammer flooded networks with a significant volume of traffic, triggering overload of routing equipment (routers). Then the cascading effect took place: since many routers became unavailable because of traffic overload, neighbouring routers from other networks started to update their routing tables, removing the unavailable ones. The flood of data on changes to the routing tables and paths caused some other routers to fail, thus exacerbating the situation. Next, another wave of traffic followed, when collapsed routers and servers were restarted by hosts owners and started to announce themselves on the network. Getting rid of the worm was quite simple and did not require any special software or scanning the infected servers: it was necessary just to close the UDP port 1434 and to restart the server.

However, over the course of its outbreak on the Internet, SQL Slammer managed to not only to affect servers themselves, but also to disrupt certain business processes and infrastructure operation. Thus, because of network overload and disabled servers 13 000 ATMs went offline in the U.S., and some of Continental Airlines online ticketing services were shut down leading to cancellation of flights.

Also, SQL Slammer accidentally induced a major disrupt into the operation of the Davis-Besse NPP in Ohio. The worm infected unpatched hosts on the network of the consulting company, which had online connection to the network of First Energy Nuclear, the licensee for Davis-Besse. After the contractor's network was also infected and started to scan IP addresses for further dissemination of the worm, Slammer paved its way directly to the process control network of Davis-Besse NPP (which also had online connection to First Energy Nuclear). Once again, the worm did not have any payload and could be targeted at ICS or any other specific IT assets. However, when infecting the hosts of the NPP's industrial network, it triggered its overload and disruption with spurious traffic. This resulted in availability of certain process control systems and devices, including the plant's Safety Parameter Display System (SPDS), radiation detectors and temperature actuators. Altogether, these systems provide to operators

important data on the condition of the NPP's reactor and indicate any abnormalities in its operation. Unavailability of data collected from these sensors in theory might make operators miss possible security incidents, including the critical ones like outage of the power plant's coolant systems or the core's overheat.

However, in this case no critical threat emerged since the Davis-Besse reactor had been taken offline in 2002 for technical maintenance. Also, the NPP had overprovisioning measures in place – digital SPDS was not the only source of sensitive data from temperature, radiation and coolant systems' detectors. The NPP's staff still was able to acquire necessary data directly from the sensors with analog output. However, unavailability of SPDS is regarded as a serious incident which should be reported if not resolved during the working shift. In the Davis-Besse case, the operation of SPDS was disrupted for approximately 4 hours.

Findings and observations:

- A key thing about Davis-Besse incident is the prominent role of cybersecurity violation and the dark side of the CNF connectivity to the Internet. Infecting the NPP's process control network with a Slammer should not have happened since the plant had an operating firewall in place, that the primitive worm would not had been able to penetrate. As the incident investigation revealed, there was a serious breach in this security policy: an undocumented connection (T1 line) was set up between the consultant's network and the NPP's business network. As the NRC filing stated, "This is in essence a backdoor from the Internet to the Corporate internal network that was not monitored by Corporate personnel", though some employees were aware of it.
- Second thing demonstrated by the incident, was weak awareness of the NPP's personnel on cybersecurity risks and ways if their mitigation. The patch to the vulnerability exploited by Slammer had not been installed at the Davis-Besse corporate network because the IT specialists did not about the patch (released 6 months before).
- The Davis-Besse incident due to its media coverage and open investigation, fueled the US public and regulatory debate on cybersecurity risks to CNF and pushed the regulators (NRC) towards elaboration of a more advanced and comprehensive regulatory framework on the matter. Open reporting and discussion became a benefit in the context of learning lessons from the incidents. At the same time, that should not be taken for granted since active discussion and investigation of SQL Slammer activities was initially triggered by its wide-scale disruptive effects on the networks countrywide, not only the Davis-Besse incident.

Case 2: The Olympic Games campaign, 2006-2012 (probably later)

CNF affected: Natanz Fuel Enrichment Plant, location: Natanz, Iran.
Incident classification: Intended / external / human factor.
Malware used: Flame, Stuxnet worm, DuQu, Gauss (and further modifications)

The information on a series of highly sophisticated cyber operations targeting the Iranian CNF, individuals and organizations involved in the nation's nuclear program is vast and detailed, but mostly not confirmed officially.

The Natanz Fuel Enrichment Plant (FEP) constructed in the first half of 2000s, was a key element in the Iranian uranium enrichment program, together with the Pilot Fuel Enrichment Plant (PFEP) located in the same underground complex. According to IAEA data, since uranium enrichment was started at the FEP in 2007, approximately 9,704 kg of low enrichment (enrichment up to 5%) was produced at the facility. According to estimates, the underground complex buildings were designed to hold altogether 50 000 centrifuges. The FEP became partially operational in early 2007, and ever after new cascades of centrifuges were intensively installed. By Fall 2009, the FEP facility was estimated to have around 4700 IR-1 centrifuges in operation, and some more in reserve or being prepared to become operational, with a total number of centrifuges installed reaching the peak of 8,692 in November.

However, it was reported that in the first half of 2009 a serious "nuclear incident" took place at the FEP that led to 30% decrease of Iran's centrifuge operational capacity and supposed shutdown of up to 1000 IR-1 centrifuges because of their physical damage. The drop in operational capacity was estimated to slowdown the Iranian uranium enrichment program for uncertain but considerable time equivalent – from 1-2 to 6 months. The fact of a major incident at the FEP was later confirmed by IAEA and the Iranian president.

Later reports and independent investigations claimed that the reason of the incident was activity of advanced computer worm known as Stuxnet. The worm was first identified in June 2009, was a highly sophisticated and selective cyber sabotage tool targeted precisely at disruption of the uranium enrichment process at FEP. Stuxnet code was of 500 KB size and contained modules for a layered attack against targeted systems, including:

- The Windows OS;
- Siemens PCS 7, WinCC and STEP7 Windows-run industrial software;
- Siemens S7 PLCs (S7-315 and S7-417).

The worm was able to spread itself across the network and had a special code piece enabling it to hide its presence on infected systems. To bypass Windows security mechanisms, Stuxnet used some previously known vulnerabilities, and also 4 zero-day vulnerabilities, an unprecedented number for an ordinary malware. To establish total control of a Windows-run system after infecting it, Stuxnet had user-mode and kernel-mode rootkit capability. That was supported by the use of 2 valid security certificates (digital signatures) that were stolen from 2 Taiwanese companies (JMicron and Realtek).

At the second layer of attack, after infecting a Windows-run system, Stuxnet searched for specific industrial applications software used by Siemens (WinCC/PCS 7 SCADA control software). This software is used to operate PLCs on industrial equipment, inter alia including CNF. If that were found on the system, Stuxnet subverted the key communication library of WinCC, which led to interception of the data flow between the software applications and the PLCs that they were supposed to run and control.

The key function of Stuxnet was revealed at layer three of the attack. In addition to targeting only two models of Siemens PLCs, the worm was also configured to target precisely frequency converters from only two manufacturers: Vacon (Finland) and Fararo Paya (Iran). There was even further stage of precise targeting: a specific piece of Stuxnet code was activated to perform cyber sabotage operation only when at layer three the malware, through monitoring infected

PLCs, was able to found motors spinning within a particular frequency range: between 807 Hz and 1210 Hz.

All those conditions were perfectly and almost uniquely met at the Natanz FEP, so the malware was initially designed and created to hit this CNF. When Stuxnet downloaded malware into Siemens PLCs at Natanz and found that they were running frequency controllers connected to motors with requested parameters (motors of the IR-1 centrifuges), the cyber sabotage sequence was activated. It was based upon repeated periodical modification of the motors' spinning frequency up to 1410 Hz (about the motors' technical limit) and then to 2 Hz, and, at the next stage, back to 1064 Hz. Resulting vibration and overload of devices led to physical damage of motors and centrifuges. According to some assessments, that might even include some components of the devices breaking apart. Since at layer two the control of data flow to Siemens SCADA control software had been intercepted, the changes in the centrifuges rotation speed were not reaching the FEP process control system and thus were not displayed to the operators. Instead, the infected PLCs commanded by the worm were continuously sending looped data showing the operation of frequency controllers within ordinary parameters. This allowed Stuxnet activities to remain undiscovered by the FEP staff for quite a long time, enough to make centrifuges connected to infected PLCs, inoperative.

There is little clarity on how Stuxnet managed to reach the Natanz FEP air-gapped industrial network back in 2009, a year before the worm accidentally leaked on the Net from an engineer's device. However, it is believed that the worm was delivered to the facility's network on some USB drive, either purposefully used by malicious insider, or purposefully infected but used by staff member unaware of it.

Later, it was discovered that several generations or versions of Stuxnet existed, so the Natanz FEP was attacked by version 1.0. In 2012, there were reports on a wave of attacks on Iranian facilities using some 1+ version of the worm – however, they did not inflict any damage comparable to 1.0. According to reports, the Iranian facilities might had been first exposed to Stuxnet threat earlier in 2008-2009, when version 0.5. of the malware was released. That one, however, was not so precisely targeted and was not able to perform the perfect cyber sabotage algorithm demonstrated by its successor at Natanz. At the same time, a peculiar moment about Stuxnet 0.5 was that the start of its creation was estimated to take place in 2005-2006, some 3-4 years before the attack on FEP was actually conducted.

In 2011-2014, in 2-5 years after the Natanz incident, a large "family" of highly sophisticated malware was revealed which is connected to Stuxnet in terms of source code, timing of its elaboration, geographic and other patterns of targeted systems, corporate entities and individuals.

In technical aspect, particular overlaps with Stuxnet included:

- The use of the same vulnerabilities in Windows-run corporate and industrial software applications.
- The use of the same security certificates (digital signatures) to bypass Windows security mechanisms.

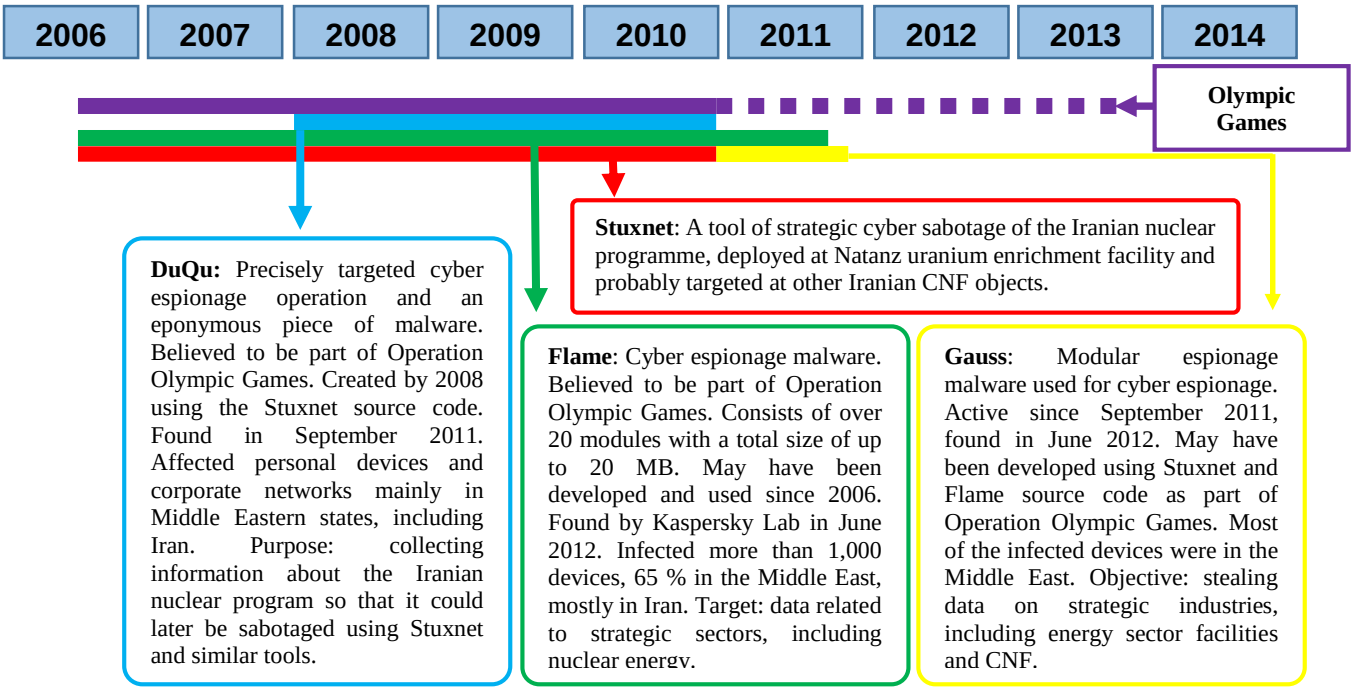
- Identical or similar pieces of source code (modified pieces of source code and specific "modules" with highly selective functionality.
- Layered attack mechanism and tools to self-erase the malware from infected systems after certain time (self-erase logic bombs).

In a broader sense, there were links as well. Many of the victims were directly or indirectly connected to the Iranian nuclear program. Iran was the prime target in terms of infections geography. The list of targets in Iran and neighboring countries of the Middle East included nuclear research institutions, security think tanks, Iranian nuclear scientists, oil&gas and banking industry companies, diplomatic institutions, research and defense corporations and agencies. However, unlike Stuxnet, these complex malwares were used not for cyber sabotage, but for highly selective and stealth cyber espionage activities, with extraction of sensitive data related to nuclear program probably being the prime goal. Among the malware identified and revealing certain connections with Stuxnet, IT-security labs and experts have mentioned Flame, mini-Flame, DuQu, DuQu 2.0, Gauss, Wiper and some others.

Finally, in 2013 media leakages and journalist investigations claimed that Stuxnet incident at Natanz FEP was a part of a grand state-sponsored cyber operation nicknamed *Olympic Games*, launched in 2005 by George W. Bush administration, later supported by Israeli Mossad and intensified by Barack Obama office in 2007-2008. The goal of the operation was to deter the progress of Iranian nuclear program without resort to military actions, e.g. bombing of Iranian CNF. Though this version never received official confirmation neither in the USA nor in Israel, is strongly coincides with the broad consensus among the expert community according to which Stuxnet and related malware was likely a part of a state-sponsored activity. Key theses in terms of this consensus are:

- Creation of Stuxnet was a resource-consuming effort that took around 4 years to develop nearly-perfect 1.0 version. Such long-terms efforts are not typical for cyber-criminal communities, who need to monetize their products. For cyber terrorists, Stuxnet and Flame were far too complex and state-of-the-art products.
- The costs of Stuxnet creation is estimated to reach or exceed 1 mln USD. In the cyber-criminal market, 1 zero-day vulnerability costs 50 000 – 100 000 USD, while Stuxnet used 4 of them. For cybercriminals, this is a very untypical way of spending money. For hacktivists and political activists, such resources are usually beyond reach.
- Precise targeting of Stuxnet undoubtedly required very deep knowledge of the Natanz FEP industrial equipment specifications, detailed knowledge of software and hardware used for the LEU production operations, as well as understanding of internal security and cybersecurity policies and procedures. Elaboration of Stuxnet 1.0 required stand testing (or some analog of) for precise calibration of its effects and finalization of the source code for Natanz operation. It would be impossible to reach that level of precision in a multi-layered attack on a very specific industrial equipment without some kind of continuous field tests.
- Start of creation of a set of cyber espionage and cyber sabotage tools targeted primarily against Iranian nuclear program (Stuxnet, DuQu, Flame, Gauss) and its lifespan quite clearly coincided with the lifespan of the US policy, aimed at deterrence of Iranian nuclear program (2005-2012).

Olympic Games lifespan



Case 3: Cyber-attacks on KHNP personnel and corporate network, December 2014

CNF affected: Korea Hydro & Nuclear Power (KHNP) corporate network, location: Seoul, Republic of Korea
Incident classification: Intended / external / human factor
Malware used: Presumably, toolkits of 'kimsuky' malware (spy programs, phishing emails with payload (exploits including droppers, malicious libraries, etc.).

Korea Hydro & Nuclear Power (KHNP), a subsidiary of the Korea Electric Power Corporation (KEPCO) operates generating facilities that provide 40% of electric power to South Korea. Among those facilities are hydroelectric plants and 4 South Korean NPPs with total of 23 nuclear reactors.

Starting from December 2014, a wave on publications emerged on the Internet, including those posted from a Twitter account of an unidentified individual nicknamed 'President of anti-nuclear reactor group". Apart from text messages, the publications contained a massive set of sensitive information related to KHNP nuclear objects. Posted information included:

- Designs and manuals of the Gori-2 and Wolsong-1 nuclear reactors operated by KHNP. Those included details on the reactors' air conditioning and cooling systems.
- Personal records on 10,799 KHNP employees, both acting and former.
- Electricity flow charts and estimates of radiation exposure among local residents in the area surrounding Gori-2 and Wolsong-1 NPPs.
- Technical information on South Korea's innovative Advanced Power Reactor 1400 (APR-1400). The reactor belongs to Generation III; at present, only one such NPP unit is in operation (Shin Kori NPP, Unit 3) and seven units under construction, including 4 in UAE.

Posting of sensitive data was accompanied with threats, blackmailing and ransom demands from unknown attacker. The hacker demanded unspecified sum of money for not releasing the rest of sensitive information he claimed to possess to third countries. He also threatened to release additional plant documents if KHNP does not comply. Finally, posts on Twitter included the threat to disrupt the operation of one of KHNP NPPs and a warning to local residents "to keep away" from the facility in next few months.

In March 2015, results of the incident's governmental investigation were announced. According to South Korean authorities, the cyber attack was committed by a group of North Korean hackers in order to stir up social unrest and agitation in South Korea. It was stressed in the reports that process control networks and ICS of KHNP's nuclear sites were beyond reach for the attackers, so the incident was limited to exposure of sensitive data only. The documents stolen in the course of the attacks were called "non-critical" for secure operation of KHNP NPPs. However, back in December, immediately after the attack, the KHNP stated in its statement that it would conduct large-scaled cybersecurity drills at 4 of its NPPs.

Investigation of the incident hardly shed light on technical details of the attack but revealed its principal algorithm. The attack was conducted in three phases.

- At phase one, the hackers used multiple Internet protocol addresses based in China to send over 6,000 phishing emails to over 3,570 former and current KHNP workers. If addressee opened the attachments to emails, malicious payload was downloaded to his device and extracted relevant data stored on it.
- Second phase included hacking of the website of the KHNP's former employees' informal online community. That was conducted using accounts of some of KHNP ex-employees that were stolen during first phase. Hacking the website allowed the attackers for extracting more data on KHNP's acting employees.
- Finally, at phase three, the attackers used all collected data on KHNP staff in order to generate and disseminate spearheaded phishing emails with malicious payload to KHNP acting employees. This was a successful step to break into the company's corporate network and steal the massive of sensitive data on its nuclear facilities and technologies.

The malware used for the attack was not pretty advanced and had nothing common with Flame, DuQu and other highly advanced cyber espionage tools from the Olympic Games case. Instead, when sending spearheaded phishing emails, the attacker used the so-called 'kimsuky" toolkits. Those include:

- The initial Trojan dropper – a Dynamic Link Library (DLL) functioning as a loader for further malware. The dropper's function is to deliver to the victim's device an encrypted malicious library equipped with espionage functionality.
- A malicious library using the Metasploit Framework's open-source code to inject malicious code and save it to the disk of the victim's device. After performing that, the library copies itself into the System32 directory of the Windows folder, creates a service for service dll. and gathers information on the device. Using a set of spying modules, the malicious service gathers and sends relevant data to the attacker.
- The malicious service disables the user's firewall and Windows Security Center service to prevent the system's security alerts.

This malware toolkit was revealed and described by Kaspersky Lab in 2013, a year before the KHNP incident. Back then, it was used to spy on and steal data from a number of South Korean think tanks and agencies, including the Sejong Institute, Korea Institute for Defense Analyses (KIDA), Ministry of Unification and Hyundai Merchant Marine.

Findings and observations:

- The KHNP incident revealed the effectiveness of primitive and well-known techniques, such as spearheaded phishing and social engineering, against professional employees of the South Korean CNF. A three-stage phishing campaign targeted at KMHP employees allowed the attackers for infecting the corporation's network and stealing sensitive data. Human factor turned out to be a major vulnerability in the environment with strong protection technologies.

- The incident and its investigation highlighted the graveness of the attribution challenge with regard to CI cybersecurity incidents. South Korean accusations of North Korean involvement were made with a three-month latency, no digital footprints or other convincing evidence was provided (except the attackers' IP addresses traced back to China) and no deterrence or diplomatic action followed with regard to Pyongyang.

- Though the incident did not inflict any damage to the KHNP NPPs operation, it might indicate a danger for a future combined attack scenario that might involve use of Stuxnet-like cyber sabotage tools and active media coverage strategy by attackers. Posting sensitive information on CNF on online media (Twitter) and threatening to conduct a cyber-attack on the NPP that would lead to a radioactive disaster did not induce panic among South Korean population, since there was no evidence that the attacker possesses any capabilities beyond stealing information. However, if attacker did succeed in hacking into the NPP's corporate network and disrupting its operation even to a minor extent, that might lead to a disproportionate reaction and provoke panic.

Case 4: Infection of the Gundremmingen NPP network, April 2016

CNF affected: Gundremmingen NPP (operated by RWE Energy AG and E.ON Kernkraft GmbH) corporate network, location: Gundremmingen, Bavaria, Germany
Incident classification: Non-intended / external / technical
Malware used: Presumably, Windows-targeting worms W32.Ramnit and Conficker

Gundremmingen NPP is currently the highest-output NPP in Germany with total generation 2688 megawatts by units B and C, which are both boiling water reactors. Due to the long-term German program of abandoning nuclear power generation, the NPP should be shut down in a middle-term future (Unit B – estimated shutdown in 2017, Unit C – estimated shutdown in 2021).

On April 7, Unit B of the NPP was temporarily taken offline for routine revision procedures that included checking and testing the facility's information systems and networks. In the

process of testing, several pieces of malware were identified and reported on April 26. In particular, the discovered malware included:

- The Conficker Worm (aka Conficker virus, Downadup and Kido), created and first discovered in 2008. The worm exploits a vulnerability in the Windows server service that was discovered and reported by Microsoft in 2008. The vulnerability is quite severe and high-impact since it allows remote code execution through Remote Procedure Call (RPC) for a number of Windows services packs, and thus could grant the attacker with remote control over infected system. In 2008, dissemination of Conficker on the Internet resulted in one of the fastest and largest worm infections since the Sasser infection of 2004. After infection, Conficker sets up an HTTP server on the infected machine and starts searching for other vulnerable devices on the network, which is a part of its strategy to disseminate itself. Control over infected system gives the operator of C&C server opportunity to extract files from it, disrupts a number of Windows services, terminates backup&security procedures and services and also disrupts access to some security-related Internet-resources. Removal tools issued by antivirus vendors are necessary to delete Conficker from the infected system.

- W32.Ramnit computer worm, first discovered and probably created in 2010. The worm spreads itself both on the Internet (using exploit kits embedded into malicious advertisements on various websites), on local networks (through infected FTP files) and offline (through removable drives). The worm targets Windows-operated systems (including Windows Server versions). However, it does not target any specific ICS/SCADA or other industrial software. W32.Ramnit is designed to serve as a backdoor, connecting to the C&C server and allowing the attacker to get remote control over the infected device once it is connected online. The purpose of the worm is to steal information with the help of multiple functional modules it has. Thus, it is able to steal files from the infected devices files, use the Internet connection sessions to steal cookies from bank and social media websites, and also conduct MITM attacks. Protection updates for W32.Ramnit were released by Symantec and other antivirus vendors back in 2010.

At the Gundremmingen Unit B network, the malware was discovered in a specific segment of the information system. In the report of the NPP operator it was stressed that the infected systems were part of the office network and have no connections to the NPP's ICS'SCADA systems or programmable field devices. At the same time, the media reports claimed that the IT systems infected with the worms were modified and retrofitted back in 2008. Since then, this segment of the NPP's network was associated with equipment for moving nuclear fuel rods.

However, industrial and process control systems (ICS/PCS) themselves were not located within the affected network segment – instead, there was some data visualization and monitoring software and/or hardware in place, undisclosed by the operator. Since both worms were not specially targeted against NPP's ICS, they were hardly able to provoke any disruption of the facility's industrial operations, including critical ones. Also, the worms could not spread beyond Windows-run server systems, since they were coded and adapted only for those ones. Finally, the network segment affected by the infection was air-

gapped from the Internet so even despite the malware tried to established undocumented connections to the Net, that did not happen. So there was not any effective opportunity for potential attackers running C&C servers to take advantage of the infection and control the worms' activities.

Initial investigation of the incident was based on the assumption that the malware traveled to the isolated network segment on some infected removable drives. Conficker and W32.Ramnit worms were identified on 18 removable data drives at the facility's office network devices, predominantly on USB sticks. This might indicate that some of the malware (Conficker worm) might have existed in the isolated network segment since 2008, when it had been modified with data visualization software.

As a result of the incident, the NPP operator announced it would enhance its cybersecurity policies and requirements. Extensive audit of the information security systems and network protection tools at the facility was conducted. Despite the fact that the operation of the NPP was not affected and the infection was occasional, the operator reported on incident to the Germany's Federal Office for Information Security (BSI). The law enforcement agency decided to join the investigation of the incident.

Findings and observations:

So far, the incident's impact has been limited to administrative and image costs for the power plant's operator. Nevertheless, several preliminary observations might be made.

- Though in general the incident reveals similarities to the Davis-Besse NPP worm infection, certain difference takes place: Conficker and W32.Ramnit are far more advanced and dangerous worms then the one that hit Davis-Besse network. Today's malware, especially Conficker, could be used for remote, covert cyber espionage operation with considerable effects. The key circumstance that prevented this scenario at the German NPP was that the malware had spread offline through removable devices, and ultimately got locked within an isolated network segment with no access to the Internet. However, a precisely targeted and well-orchestrated attack on NPP's Internet-connected office network with the use of Conficker and W32.Ramnit might reach its goal and lead to loss of sensitive data. The level of information security hygiene revealed by the incident is low enough to consider this as a feasible option. However, all speculations about the worms potentially affecting the nuclear fuel rods transportation in this case should be regarded as unfounded alarmism.

- Modifications of the CNF network segmentation and architecture might create new vulnerabilities in the defense perimeter of the ICS layer. Since there are no standard solutions and each CNF in terms of its networks is a project in a class of itself, potential risks of any retrofitting or modification should be precisely assessed and calculated. Proper division between different functional segments of the CNF network (office and administrative – ICS/process control) should be a priority. That might have been to some extent neglected or underestimated at the Gundremmingen NPP in 2008, since a segment of the office network was connected to data visualization systems linked to critical nuclear fuel transportation operations.