Confidential

RUSSIA

**The circulation of this report is strictly limited to members of the *Trialogue* Club International
and of the Centre russe d'études politiques.**

This issue is for your personal use only.

**Published monthly in Russian and in English
by *Trialogue Company Ltd.***

Issue № 12 (240), vol.15. 2016

December 27, 2016

Oleg Demidov reports from Moscow:

CYBER ATTACKERS KNOCKING ON *NUCLEAR DOOR* IN CIVIL REALM*:*

RUSSIAN VIEW ON HOW TO MITIGATE THE THREAT

SUMMARY

Operators of critical infrastructure (CI) all over the world are facing increasing cyber risks. The danger is coming not from accidental software and hardware failures or human factor as it used to be. The threat focus is shifting towards purposeful cyber-attacks on CI, conducted by skillful actors with both criminal and policy motivation.

The bad news is that fundamental technology trends play into greater vulnerability of critical facilities' IT infrastructure. Critical infrastructures become increasingly connected – that is an inevitable trend dictated by optimization of business processes. Its dark side is a front door of critical facilities open wide for cyber intruders.

A particularly bright illustration for these trends among all critical sectors represent peaceful nuclear installations which are a new target No.1 for advanced actors in cyberspace, argues PIR Center's consultant Oleg Demidov, an expert on cybersecurity issues.

In this issue of Russia Confidential, Russian expert explains the reasons behind special vulnerability of nuclear facilities to cyber threats and identifies ways to mitigate them, whereby he highlights the analytical effort of PIR Center, one of the leading Russian think tanks working in this area.

CYBER THREATS TO PEACEFUL NUCLEAR FACILITIES: *GENIE OUT OF THE BOTTLE*

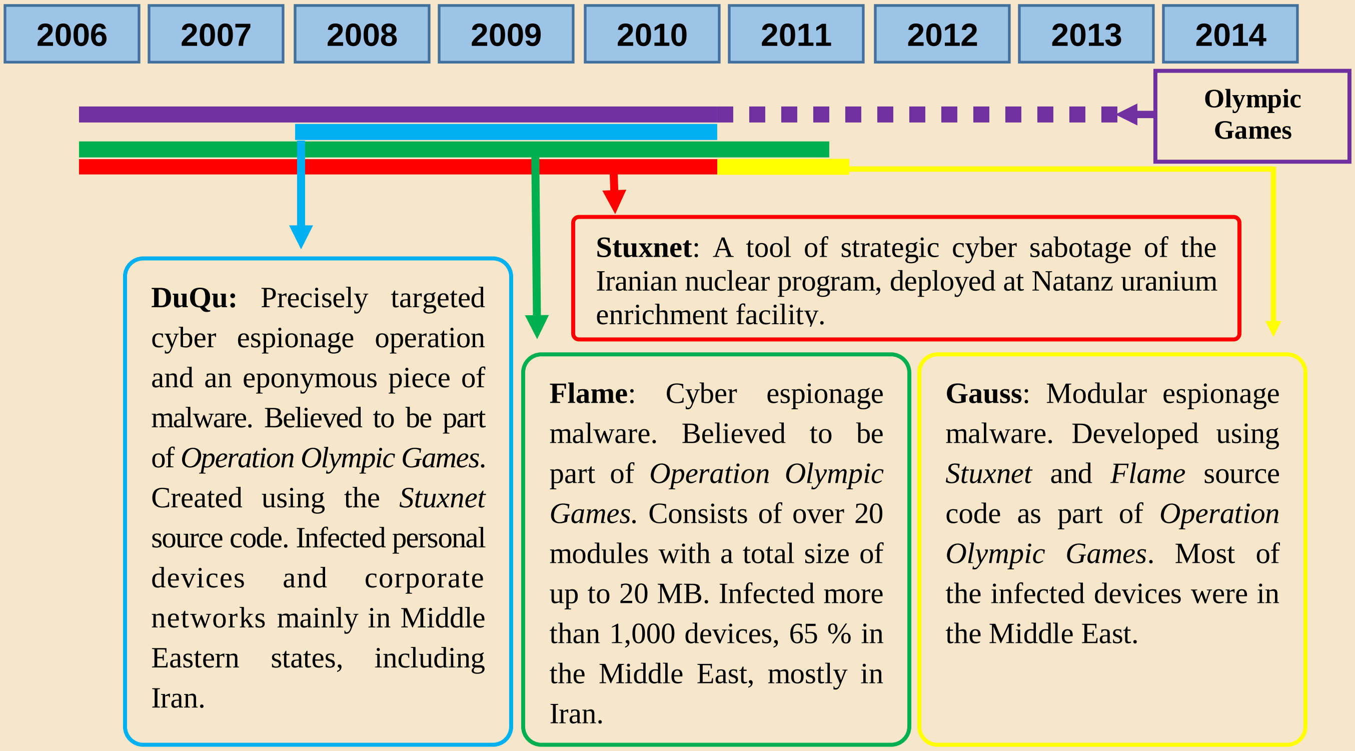
Peaceful nuclear installations became targets for malicious cyber activities already in a number of countries. Prominent cases include worm infection of the *Davis-Besse* nuclear power plant in the U.S. in 2003, *Stuxnet* and the *Olympic Games* operation in 2005-2012 (see Chart 1), cyber-espionage campaign against South Korean KHNP power plant operator in December 2014, and worm infection of the Gundremmingen power plant in Germany in April 2016. The list is to be continued, as basic observations from those incidents suggest:

- ***Damage threshold for targeted assets has drastically increased. State-of-the-art cyber weapons directly target field devices and are designed for full-scale cyber sabotage operations. A notorious example is Stuxnet.***

- ***Revealing and investigating the incident might not be enough to displace the threat, because attackers' tools are easily modified and re-used.***

- ***Threat vectors drift from traditional ones and include attacks on third parties, social engineering, and other innovative techniques.***

Putting it in simple words, the genie is now out of the bottle.



DuQu: Precisely targeted cyber espionage operation and an eponymous piece of malware. Believed to be part of *Operation Olympic Games.* Created using the *Stuxnet* source code. Infected personal devices and corporate networks mainly in Middle Eastern states, including Iran.

Stuxnet: A tool of strategic cyber sabotage of the Iranian nuclear program, deployed at Natanz uranium enrichment facility.

Flame: Cyber espionage malware. Believed to be part of *Operation Olympic Games*. Consists of over 20 modules with a total size of up to 20 MB. Infected more than 1,000 devices, 65 % in the Middle East, mostly in Iran.

Gauss: Modular espionage malware. Developed using *Stuxnet* and *Flame* source code as part of *Operation Olympic Games*. Most of the infected devices were in the Middle East.

Chart 1. The *Olympic Games* campaign lifespan.

Several **technological trends** are changing the way IT infrastructures evolve in the peaceful nuclear energy sector.

➢ First, online connectivity now goes beyond corporate and office networks of power plants and enrichment facilities. Field devices that enable operation of critical industrial processes of nuclear facilities are digitalized and connected online too. Another connected segment includes sensors and actuators installed at industrial equipment, monitoring its performance and sending data to parameter monitoring systems. However smart and convenient, those systems and devices are becoming too numerous and hard to integrate in a secure way.

- Second, corporate and office segments of nuclear facilities' networks are widely connected to the Internet for a smoother exchange of data with external contractors, consultants, etc.
- These trends are accompanied by *mobile revolution*, growing market of remote online services for managing industrial control systems over the Internet from one's mobile device (*SCADA in your pocket*). These innovations extend the network defense perimeter and create new potential pathways for attackers.

Though these trends are common to all critical infrastructures, peaceful nuclear facilities are a remarkable case. Each NPP has hundreds of industrial control systems and tens of thousands of detectors and actuators, so profound consequences are inevitable:

- ***Complexity of nuclear installations limits the applicability of previous experience and best practices in terms of ensuring cybersecurity.***
- ***Huge number of critical IT components make operators depend on too many vendors; besides, it is almost impossible to ensure integrity of supply chains.***
- ***Standard cybersecurity approaches are not enough. Advanced strategies are needed, such as cybersecurity by design, real-time event management, deployment of cryptography on industrial networks. Those are hard to be put in place instantly, without big longer-term investments and regulatory debates.***

TAKING THE CHALLENGE NATIONALLY AND INTERNATIONALLY

National governments are making some efforts to mitigate cyber threats to peaceful nuclear facilities, but these are largely dragging behind the evolution of threats.

- In most countries cybersecurity of nuclear facilities is just emerging as a separate regulatory framework, with a number of issues slowing the process down. Those include ambiguity in division of regulatory agenda between governmental agencies, 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.
- Another issue is lack of a single sector-specific regulator that often leads to weak feedback from private sector stakeholders. Rigid nuclear security paradigm sometimes acts as a barrier to elaboration of a hybrid regulatory framework addressing specific issues of the civil nuclear sector. Finally, proper integration of international guidelines, recommendations and best practices into national regulations is often missing.

On the **international** level, mitigation of cyber-attacks on nuclear installations faces legal vacuum. No international mechanisms aimed at countering and preventing such acts are in place. Sensitiveness and national security considerations make this agenda fall out of the scope of anti-cybercrime frameworks, such as the

Convention on Cybercrime adopted by the Council of Europe in 2001. One format which is trying to address cyber protection of critical infrastructures is the **United Nations Group of Governmental Experts on cybersecurity**. Yet, their proposals to nation states are put as voluntary non-binding norms and do not address nuclear installations directly.

In these circumstances, best efforts are made by **IAEA** that provides technical guidelines, trainings, capacity building and awareness raising activities on computer security of nuclear facilities.

Still, 90% of the work is definitely ahead. Before drafting norms, world leaders have to at least elaborate a shared taxonomy for cyber threats to nuclear energy sector.

The good news is that the **UN** is casting its glance to mitigation of cyber challenges to nuclear facilities increasingly often and purposefully. In July 2016, the Report of the Secretary General based upon the Work of Advisory Board on Disarmament Matters (ABDM) was published. In the document, the Board stressed the potential threat of terrorists using cyber means to cause death, destruction and disruption on a scale comparable to the use of CBRN weapons, and proposed to the Secretary General to highlight the issue on coming international forums.

RUSSIAN *THINK TANK* CONTRIBUTION: PIR CENTER'S WORK ON THE ISSUE

Apart from the industry, governments and international bodies, considerable efforts to address the issue and to identify solutions are made by the expert community. One of such efforts was launched by a leading Russian non-governmental *think tank* – the **PIR Center**.

- In Spring 2016, PIR Center published its report "*Cybersecurity of Civil Nuclear Facilities: Assessing the Threat, Mapping the Path Forward*" which benefitted from consultations with leading experts in Moscow and Geneva. The research paper provides a reference model for cyber threats to nuclear infrastructure (see Chart 2 on the next page) and a three-level vision for future steps for industry, regulators and international fora.

On **technical level**, new approaches need to be put in place, primarily through collaboration of operators and IT vendors. To eliminate backdoors in critical equipment, penetration- and fuzz testing, deep scanning of programmable field devices firmware is required. More intense exchange of experience and best practices between leading IT vendors and cicil nuclear facilities operators might be helpful. Operators could benefit from adopting cybersecurity by design and deployment of cryptographic tools in their industrial networks. For nuclear power plants, disclosure of the field devices' source code to operators might be a viable option.

On **regulatory level**, s priority goal should be deeper integration of cybersecurity into nuclear security paradigm in order to eliminate functional gaps and overlaps between cyber and nuclear regulators. To achieve that, internal dialogue among national regulators should be intensified and promoted by governments and supported with comprehensive legislation on nuclear cybersecurity. Here, IAEA's role remains instrumental in terms of accumulating best practices from advanced states and providing reference models for developing ones. Governments also have to breed a generation of cybersecurity specialists with a new mindset, able to complement and enhance traditional nuclear security approach. That requires innovations in the higher education system and support of trainings, workshops and dialogues involving both nuclear and IT industries.

Internationally, the UN Group of Governmental Experts' work could be helpful for resolving the taxonomy, terminology and classification of critical nuclear infrastructures and cyber threats to them. Meetings of the 5th Group in 2017 might contribute to shaping shared vision on the issue, if its new report would directly address cyber protection of nuclear installations and contain proposals for non-binding norms. Some of earlier Group's proposals could be updated to address the issue ensuring the integrity of supply chains for critical IT systems procured to nuclear operators.

Even though making the *genie of cyber threat* go back into the bottle is rather unrealistic, concerted efforts on those three policy levels might help the global nuclear energy industry to effectively mitigate the threat.

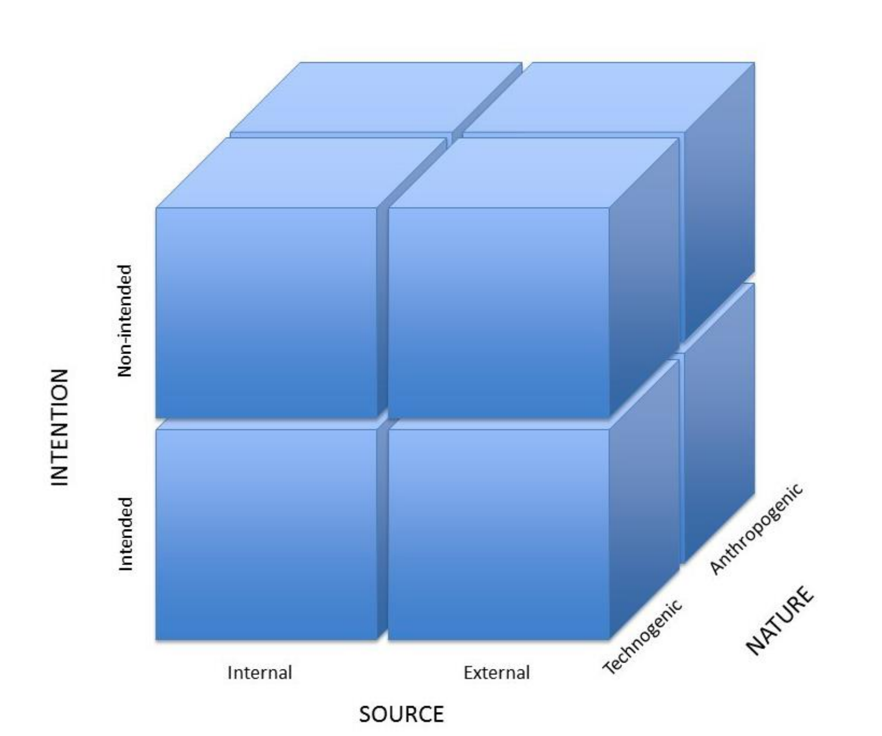


Chart 2. Basic reference model for cybersecurity incidents on civil nuclear facilities. *Source:* PIR Center

The author of this article is Oleg Demidov – PIR Center consultant,
expert on cybersecurity issues

Editor: Julia Fetisova

Moscow – Geneva, December 2016

Excerpts from the Membership Terms and Conditions at the Trialogue Club International

3. Club members' rights

3.1. Individual members of the Club have the right to:
3.1.3. Receive one copy of the Russia Confidential exclusive analytics bulletin by email, in their preferred language (Russian or English). Under the rules of the Club, the bulletin may not be made available to third parties. […]
3.2. Corporate members of the Club have the right to:
3.2.3. Receive two copies of the Russia Confidential exclusive analytics bulletin by email, in their preferred language (Russian or English) or in both languages, and to make the bulletin available to other representatives of the corporate club member. Under the rules of the Club, the bulletin may not be made available to third persons who are not members of the Club.
[…]

4. Club members' responsibilities

4.1. All current members of the Club have the following responsibilities:
4.1.6. Not to share materials from the Russia Confidential bulletins they have received, or passwords to the Club website, with individuals and/or entities who are not members of the Club.
[…]

6. Russia Confidential

6.1. The Russia Confidential exclusive analytics bulletin is published by OOO Trialogue for personal use by Club members only.
6.2. The bulletin contains concise and exclusive analysis of problems pertaining to international security and Russian and CIS domestic and foreign policy issues, written specially for Russia Confidential by leading experts.
6.3. Materials published in the bulletin should be treated as confidential for at least 30 days from the date of publication. During that period they may not be quoted or made available to persons or entities who are not Club members.
6.4. After a period of at least 30 days from the date of publication, OOO Trialogue may choose to lift the exclusivity and confidentiality requirements for some of the materials published in the bulletin, in which case they may be published in other outlets and quoted by Club members.
6.5. The bulletin is sent to Club members by email on a monthly basis, in English or in Russian, depending on the individual club member's preference.
6.6. Upon request, Club members can also receive a hard copy of the bulletin in their preferred language.

Dear members of Trialogue Club International,

The year 2016 is drawing to a close, and we kindly **invite you to extend your membership of the Club for 2017 or for the 2017-2018 period.**

In 2017 Club members will continue to receive exclusive analytics on Russian foreign policy priorities and key challenges and threats to international security. We have scheduled **5 meetings of *Trialogue* Club International** in 2017, including 4 in Moscow and 1 abroad. Club Members will receive a series of articles from the Security Index journal in electronic form, **12 issues** of the Russia Confidential analytical bulletin (in Russian or English), as well as other information and analytical bulletins.

As always, specialists of *Trialogue* Club International and its partner organization PIR Center are open for exchange of opinions on key international issues.

Club membership in 2017

If you renew your membership before **December 30, 2016**, membership fees are as follows:

Period	Individual	Corporate
01.01.17 – 31.12.17 (1 year)	45 000 roubles	72 000 roubles
01.01.17 – 31.12.18 (2 years)	81 000 roubles	126 000 roubles

If you renew your membership before **January 31, 2017**, membership fees are as follows:

Period	Individual	Corporate
01.01.17 – 31.12.17 (1 year)	50 000 roubles	80 000 roubles
01.01.17 – 31.12.18 (2 years)	90 000 roubles	140 000 roubles

We operate a **1+1 arrangement** for **corporate members**, whereby each corporate member is entitled to have **2 representatives** participating in Club events.

For all membership issues, please email us at secretary@trialogue-club.ru or call +7 (985) 764-98-96.

Sincerely,

Chairman,
***Trialogue* Club**
International

Dmitry Polikanov

Confidential