WORLD ECONOMIC FORUM

Our nuclear facilities are increasingly vulnerable to cyber threats. This is what policy-makers need to know

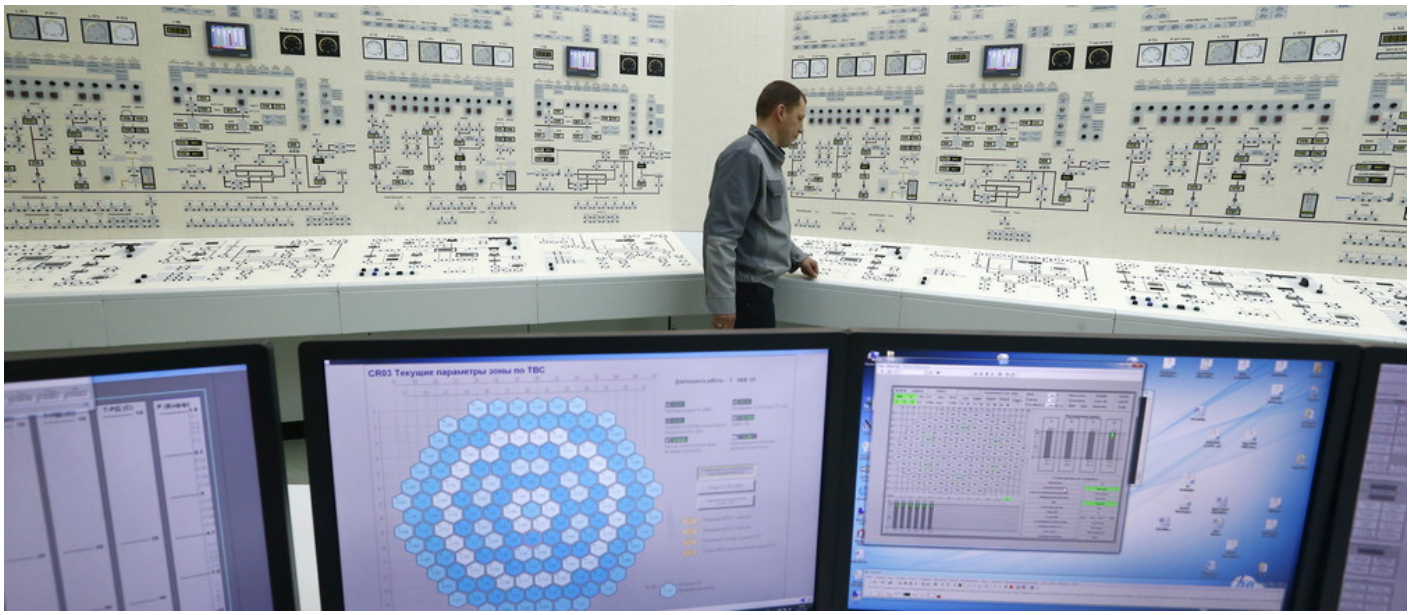

Image: REUTERS/Vasily Fedosenko

05 Oct 2016

Vladimir Orlov
Executive Board Member, Special Advisor, PIR Center

All over the world, operators of critical infrastructure face increasing cyber risks. The danger is coming not from accidental software and hardware failures, or from human error, as was the case in the past. The threat is now intentional cyber-attacks on critical facilities, conducted by skillful actors with both criminal and political motivations.

Of all the infrastructure that could potentially be targeted by such intruders, peaceful nuclear installations are one of the biggest cause for concern.

Learning from past incidents

In fact, there have already been a number of high-profile cases where this has happened, such as the worm infection of the David-Besse nuclear power station in 2003, a cyber-espionage campaign against South Korea's KHNP power plant operator in December 2014, and a worm infection of the Gundremmingen power plant in Germany in April 2016.

What have these incidents taught us so far? For one, we now know that the 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.

We also know that revealing and investigating incidents might not be enough to displace the threat, because attackers' tools are easily modified and re-used.

Finally, these incidents have demonstrated that the nature of the attacks is also changing: threat vectors drift from traditional threats and include attacks on third parties, social engineering techniques and other innovative methods.

Why are nuclear power plants so vulnerable?

Several technological trends are changing the way IT infrastructure evolves in the peaceful nuclear energy sector.

As in other industries, the corporate side of a nuclear facility is widely connected to the internet. While this helps manage relationships with external contractors and consultants, for example, it also extends the network defense perimeter, and creates new opportunities for attackers to exploit.

Today, though, online connectivity goes far beyond a plant's corporate and office networks – now, field devices to operate critical industrial processes are also digitalized and online. So too are the sensors and actuators used for monitoring a plant's performance and sending data to parameter monitoring systems. However smart and convenient, those systems and devices risk becoming too numerous and hard to integrate in a secure way.

Though these trends take place among all critical infrastructures, civilian nuclear facilities are unique in that each plant has hundreds of industrial control systems and tens of thousands of detectors and actuators. This complexity limits how much cybersecurity best practice from other industries can be applied.

The huge number of critical IT components also means that operators depend on a large

number of vendors, making it almost impossible to ensure the integrity of supply chains.

In the case of nuclear facilities, standard cybersecurity approaches are not enough. Advanced strategies are needed, such as cybersecurity by design, real-time event management, and deployment of cryptography on industrial networks. For those to happen, we'd first need regulatory debates and long-term investments.

Are regulators ready to mitigate the challenge?

Governments are making some efforts, but on the whole the threats themselves are evolving too fast for them to keep up.

In most countries, the cybersecurity of nuclear facilities is just emerging as a separate regulatory framework, with a number of issues – including a lack of clarity as to which department manages what, and in many cases some overlap – slowing down the process.

For the same reasons, few countries have a single sector-specific regulator, which often hinders feedback from the private sector. They have also, so far at least, failed to integrate international guidelines, recommendations and best practices into their national regulations.

Taking the challenge internationally

Up on the international level, we're met with a legal vacuum: no international mechanisms aimed at countering and preventing such acts are in place. Because of how sensitive this topic is, and because of national security considerations, this issue falls out of the scope of anti-cybercrime frameworks.

The United Nations Group of Governmental Experts on Cybersecurity has been a step in the right direction, but its proposals to nation states are voluntary and non-binding, and do not address nuclear installations directly.

It's not the first time the UN has attempted to intervene in this area. In July 2016, a report from the UN secretary-general based on the work of the Advisory Board on Disarmament Matters was published. In the document, the board stressed the potential for terrorists to use cyberattacks to cause death, destruction and disruption on a scale comparable to CBRN weapons, and called on the secretary-general to highlight the issue at upcoming international forums.

Have you read?

Is the nuclear security threat growing?

How can we push for tighter security for nuclear weapons?

Think the nuclear threat ended with the Cold War? You're wrong

---

In these circumstances, the International Atomic Energy Agency should focus on providing technical guidelines, trainings, capacity building and awareness-raising activities about computer security at nuclear facilities.

Still, the majority of work is ahead of us. Before drafting norms, world leaders must first decide on a shared taxonomy for cyber threats in the nuclear energy sector.

The future of nuclear security

On a technical level, new approaches need to be put in place, primarily through collaboration of operators and IT vendors. To eliminate backdoors in critical equipment, we need to focus on penetration and fuzz testing, and deep scanning of programmable field devices firmware. More knowledge sharing between IT vendors and nuclear operators might also be helpful. Operators should look at adopting cybersecurity by design and deploying cryptographic tools in their industrial networks. For nuclear power plants, we should also consider disclosing the field devices' source code to operators.

Another strategic goal could be the deeper integration of cybersecurity into the nuclear security paradigm, 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, the International Atomic Energy Agency's role remains instrumental in terms of accumulating best practices from advanced states and providing reference models for developing ones. At the national level, we need a generation of cybersecurity specialists with a new mindset, able to complement and enhance the traditional approach to nuclear security. That requires innovations in higher education and the creation of trainings, workshops and dialogues involving both the nuclear and IT industries.

Internationally, the work of the UN Group of Governmental Experts could be helpful for

resolving the taxonomy, terminology and classification of critical nuclear infrastructures and cyber threats. Meetings of the Fifth Group in 2016-2017 might contribute to shaping a shared vision on the issue, if its new report directly addresses the cyber protection of nuclear installations and contains proposals for non-binding norms.

It is too late, too unrealistic to expect that the cyber threat genie will go back into the bottle. Yet concerted efforts on those three policy levels might help the global nuclear energy industry to effectively mitigate and minimize the threat.

This post is based on research carried out for a report from the PIR Center in consultation with members of the Global Agenda Council on Nuclear Security, Cybersecurity of Civil Nuclear Facilities: Assessing the Threat, Mapping the Path Forward

Written by

Vladimir Orlov, Executive Board Member, Special Advisor, PIR Center

New report: Top 10 Emerging Technologies of 2019