The Cyber Threat to Nuclear Facilities: Frequently-Asked-Questions

What are the potential consequences of a cyberattack on a nuclear facility?

Cyberattacks on civilian nuclear facilities can be considered in three broad categories: those that target business networks, access control systems, and industrial control systems (ICS) - including security and safety systems. Cyberattacks on nuclear facilities can have consequences ranging from minor to potentially catastrophic.

- Attacks on business networks may result in the theft of sensitive data that could be used for blackmail or financial gain. Attackers may also choose to enter the business network as a means to gain access to the control systems and/or lay the groundwork for a future attack.
- Theft of nuclear material may occur as a result of an attack on access control systems (including physical protection, control, and/or accounting systems). For example, an attacker could hack into a badge permissions system to gain access to restricted parts of a facility where nuclear material is kept, and then compromise materials accounting systems to hide the theft.
- Attacks on ICS (e.g., digital systems that control sensors, valves, heaters) can range from minor to potentially catastrophic. Minor effects may go unnoticed or initially be difficult to attribute to a cyberattack. Attacks could be so severe as to disable cooling systems, which could result in the release of radioactive material on a Fukushima-like scale in a worst-case scenario.

Have nuclear facilities been subject to cyberattacks?

Yes, although it is difficult to know the frequency, as cyber security incidents at nuclear facilities are often not publicly disclosed. Known recent examples, however, include: destruction of centrifuges at the Iranian Natanz nuclear facility due to Stuxnet, data theft at the Korea Hydro and Nuclear Power Company in South Korea, and the recent disclosure of computer viruses in the Gundremminger nuclear power plant in Germany.

Do existing safety and security measures already provide protection from cyberattacks?

In many cases, existing safety and security measures do provide some protection from cyberattacks, especially in facilities utilizing analog safety or security systems. Nuclear facility engineers and operators, however, must consider not just what systems are *designed* to do, but what they can be *made* to do. For example, safety systems typically guard against single,

naturally occurring failures. An adversary could circumvent this by causing multiple simultaneous failures with a cyberattack—an outcome for which systems were not designed.

What measures should countries and nuclear facilities take to protect themselves from cyberattacks?

In order to protect themselves, nuclear facilities must recognize the implications of cyberattacks on nuclear facilities, and then work to secure their systems and networks. This involves implementing industry best practices as they are developed, training personnel, and working with vendors to utilize more secure technologies. In addition, facilities can and should make use of existing resources, such as those provided by the International Atomic Energy Agency (IAEA) and the Nuclear Energy Institute (NEI), to achieve these goals.

At the regulatory level, national nuclear regulators should develop, implement, and ensure compliance with robust cyber security regulations. Over the longer term, countries need to develop more ambitious strategies to keep pace with the cyber threat. These strategies should be constructed around four key priorities: institutionalizing cyber security at nuclear facilities, implementing active defense postures to respond quickly when breaches occur, reducing complexity within computer networks and systems, and supporting transformative research to develop hard-to-hack systems for critical applications.

What international organizations are involved in addressing this issue?

Many international organizations are involved in addressing cyber security at nuclear facilities. The IAEA develops and publishes high-level cyber security guidance and provides hands-on training workshops to Member States. Cyber security at nuclear facilities was discussed within the Nuclear Security Summit (NSS) process; at the 2016 Summit, 29 countries and the United Nations signed a Gift Basket titled *Cyber Security of Industrial Control and Plant Systems at Nuclear Facilities*. At the 2016 Nuclear Industry Summit (an official side event of the 2016 NSS), participants agreed to undertake actions to improve the state of cyber security across all nuclear facilities and applications beyond 2016. Additionally, the United Nations Group of Governmental Experts (GGE) produced a report in 2015 recommending norms in cyberspace, as well as international cooperation and capacity-building. Finally, the World Institute for Nuclear Security (WINS), the World Nuclear Association (WNA), the World Association of Nuclear Operators (WANO), NEI, and the Organization for Security and Co-operation in Europe (OSCE) are also working to address the issue.