THE CENTER
FOR ARMS CONTROL
AND NON-PROLIFERATION

Ask an Expert: Des Browne on Nuclear Cyber Security

Lord Browne of Ladyton (Des Browne) has been serving as Nuclear Threat Initiative's (NTI) Vice Chairman since 2014. He also serves as Chair of the European Leadership Network. Formerly, he was a Member of the British Parliament for Kilmarnock and Loudoun from 1997 to 2010. Lord Browne was appointed Secretary of State for Defence in 2006 and from 2007 to 2008, he served as the Secretary of State for Scotland. From 2009 to 2014, he served as Convenor of the top level group of parliamentarians for multi-lateral nuclear disarmament and non-proliferation.

In this interview, Lord Browne provides an overview of cyber threats to nuclear weapon command, control and communications systems in the United States and abroad, outlines the safeguards in place to address cyber vulnerabilities, and stresses the importance of organizations like the International Atomic Energy Agency (IAEA) in monitoring threats to nuclear materials and industry.

1. Are U.S. nuclear weapon command, control and communications vulnerable to a cyber-attack?

   Nuclear weapons and related systems are among the most highly secured systems. That said, it is not possible to provide 100% assurance that any computer-based system is not vulnerable to attack. Given the potential consequences of an attack on a nuclear weapon or related system, all responsible governments need to consider the full range of technical, procedural and policy solutions to minimize the risk.

A) What safeguards are in place to protect U.S. nuclear command, control, and communications from potential cyber threats?

   Specific security procedures are, and should be, highly confidential. It is publicly known, however, that systems are isolated from the public internet, that redundant warning systems are in place and that specific codes must be provided in order to arm and launch nuclear weapons.

B) The United States is undertaking an extensive plan to rebuild all three legs of the U.S. nuclear triad and its associated weapons and infrastructure. Will this rebuild increase the vulnerability of the U.S. nuclear arsenal to cyber threats?

   Renewing the triad will undoubtedly involve use of modern technology, which is increasingly digital and which presents greater exposure to the potential for cyberattacks. Although the government plans to address cyber vulnerabilities through modernization, new vulnerabilities could be introduced.

   Cyberattacks could occur during development or production by compromise of the supply chain, or when in use, for example, by a malevolent insider. As for any critical system, the US government needs to consider the importance of cybersecurity when implementing new technologies, and whether there might be benefits to retaining some “old” and less cyber-vulnerable technology or keeping a “person in the loop” to mitigate against the cyber risk.

2. A recent report released by NTI documented the risks of cyberattacks on nuclear facilities. What is one thing the public and decision makers should know about this threat?

   The NTI report highlights the potentially catastrophic consequences of a cyberattack on a nuclear facility--for example, a power plant.

   What is unnerving is that cyber incidents are already happening and at an increasing pace. The report provides a list of 23 cyber incidents at nuclear facilities since 1990--including a 2014 attack that resulted in the theft of blueprints and manuals for two nuclear power plants from a South Korean company which operates 23 of the country’s nuclear reactors. Reading the report, it becomes clear that attempts to address cybersecurity at nuclear facilities is not equal to the challenge.

Of course, levels of preparedness vary greatly around the world. The report outlines four overarching priorities that we believe will allow countries to get ahead of the growing threat.

Both public and decision makers should know that while there are stringent safety regulations for nuclear power plants and other nuclear facilities, addressing cyber risks has not caught up in most parts of the world. Responding to this threat is a long-term effort that involves industry, government and international organizations working in new, more dynamic ways.

These systems are enormously complex. This complexity makes it impossible to provide complete confidence in the security and to even understand the full implications of an attack. Because of this, any solution must take this into account while working to reduce complexity to the extent possible.

3. NTI's Nuclear Materials Security Index highlights nuclear facilities and stockpiles of nuclear material scattered throughout the world, many poorly protected from physical and cyber threats.

A) Are these threats being taken seriously by the countries where these facilities are located? By the U.S. government? By the international community?

Overall, most countries and certainly the United States and United Kingdom take the security of nuclear materials and facilities very seriously. And in large part, we have former President Obama and the host countries for the series of Nuclear Security Summits to thank. While this issue is taken seriously, there continue to be challenges caused by weak regulatory systems, bureaucratic inertia and broad issues such as corruption.

B) What can the U.S. and international community do to mitigate these threats?

The final Nuclear Security Summit was held in 2016, so it will be critical to focus attention on this issue and to continue to make progress. This is particularly true for emerging issues, like the cyber threat posed to nuclear facilities.

C) Is there adequate funding for international organizations that work to mitigate the threat of nuclear security breaches?

Funding is always a challenge for individual governments, particularly outside of the U.S. Support for the IAEA is critical. Although the IAEA is the closest thing the world has to a global nuclear watchdog, it requires growing resources and authority to do its job, in light of expanding responsibilities (like the Iran agreement) and the dynamic threat environment (like cyber). Today, the IAEA does not currently have adequate human or financial resources to significantly expand its existing responsibilities, like peer review services for member states.

To learn more about cyber security at nuclear facilities, read NTI's report Outpacing Cyber Threats and for more on the security of nuclear materials around the world, read NTI's Nuclear Materials Security Index.