Please find below a response to the question on notice about cyber security and attacks on nuclear facilities.

Professor Ruff will respond in regard to the other two questions.

Yours sincerely

Margaret Beavis

The cyber threat has expanded dramatically in recent years, with a series of damaging, high-profile attacks that have made headlines around the world. Nuclear facilities and critical command and control systems are not immune to cyber-attack—such an attack could facilitate the theft of weapons-usable nuclear materials or a catastrophic act of sabotage.

According to Yukiya Amano, director general of the International Atomic Energy Agency (IAEA), at the International Conference on Computer Security in a Nuclear World Vienna, June 1st 2015, nuclear facilities around the world are facing daily cyberattacks on their systems:

"*Reports of actual or attempted cyberattacks are now virtually a daily occurrence. Last year alone, there were cases of random malware-based attacks at nuclear power plants and of such facilities being specifically targeted … staff responsible for nuclear security should know how to repel cyber-attacks and to limit the damage if systems are actually penetrated. The IAEA is doing what it can to help governments, organizations, and individuals adapt to evolving technology-driven threats from skilled cyber adversaries".*[1]

In addition to the threat of external cyber-attack, deliberate sabotage by operating staff or others is also possible. There have been a number of airline mass deaths due to deliberate pilot decisions, presumed to be due to mental illness. The most recent of these was the Germanwings crash in 2015. These types of attack are extremely difficult to prevent.

Indeed in an article titled "Is the United Kingdom's nuclear arsenal safe from cyberattack?" for the European Leadership Network, Dr. Andrew Futter, an associate professor of international politics at the University of Leicester in the United Kingdom observed:

"*Humans and the human-computer interface are often the easiest target and biggest security risk in cyber operations.*"[2]

The Chatham House International Security Programme notes:

"*The exploitation of cyber vulnerabilities in critical infrastructure is becoming an increasingly pervasive security threat. At the global level, dependence on cyberspace is increasing and creates new and unexpected vulnerabilities. This dependence extends to nuclear energy production plants, which rely on computer networks for most internal processes. Many plants are connected to external networks, and there are a variety of ways in which a malicious actor could exploit these dependencies to create a security incident*.[3]"

QONs_Dr Margaret Beavis, Medical Association for Prevention of War (Australia)

The Nuclear Threat Initiative, a Washington-based non-profit co-founded by Ted Turner, has tallied about two-dozen cyber incidents 1990-2016, at least 11 of which were malicious[4].

Any list of cyber incidents in the nuclear sector, however, is very likely incomplete. The US Nuclear Regulatory Commission, for example, only requires operators to report to the commission cyber incidents that affect the safety, security functions, or emergency preparedness of the plant, excluding potentially significant attacks on IT systems[5].

1. https://www.iaea.org/newscenter/statements/remarks-international-conference-computer-security-nuclear-world-vienna-june-1-2015
2. https://www.nti.org/analysis/atomic-pulse/cyber-threats-nuclear-weapons-should-we-worry-conversation-dr-andrew-futter/
3. https://www.chathamhouse.org/about/structure/international-security-department/cyber-and-nuclear-security-project
4. www.nti.org/media/documents/NTI_CyberThreats__FINAL.pdf
5. https://www.theverge.com/2018/1/23/16920062/hacking-nuclear-systems-cyberattack