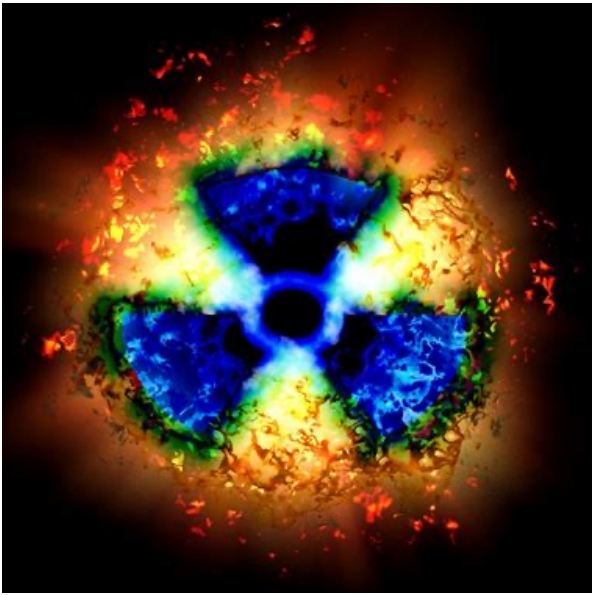


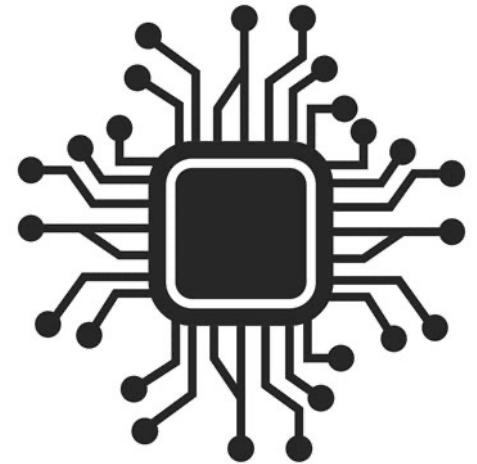
The Issue of the Risk of Cyberattacks on Nuclear Weapons Arsenals



With the growing use of digital security to protect and use nuclear weapons, cyberattacks have increased in their risks and danger. Cyberattacks could potentially disrupt weapons systems, causing unintended consequences, such as disengaging weapons to prevent them from use, or releasing weapons with harmful consequences. The definition of a cyberattack is an unauthorised attempt by hackers to damage, destroy, steal, alter, disable or expose data or computer infrastructure. The exposure of a country's nuclear arsenal could leave them vulnerable to physical attacks, and leave them defenceless. Cyber attacks can also be used defensively by a country, to prevent missile strikes, which has benefits such as reducing the need for air defence systems, which are costly and single use.

While a country may use cyberattacks strategically, an issue arises from third party hackers causing havoc with unprecedented attacks. This has the potential to cause disputes between countries, as well as disable a country's nuclear program, or cause a country to use nuclear weapons without meaning to. A heavily networked system is more vulnerable to cyber attacks, and these could go undetected, such as in the case of the Stuxnet worm, which sabotaged the Natanz uranium enrichment plant for years without detection.

Cyberattacks can reduce second strike capabilities for a country, reducing its strategic stability. Without nuclear weapons to counter a first attack, this increases the incentive to strike that country, as there will be no counter strike. This can lead to a state releasing their nuclear weapons if they believe they have been breached, or creating separate nuclear weapons programs to ensure that in case of attack, nuclear weapons are still available. However, this can be seen as aggressive, and cause other countries to counter this with their own expanding nuclear programs, leading to dangerous competition for arms.



Cyberattacks can destabilise a state's nuclear security, and have the potential to cause havoc to governments and threaten life. With the growing threat nuclear weapons pose, it is essential that they do not fall into the wrong hands, or be used in a harmful way as a result, so effective solutions are needed to prevent deadly cyberattacks.

Points to consider:

- How can the UN ensure that the threat of cyberattacks on nuclear arsenals is neutralised?
- Should cyberattacks and nuclear weapons be less classified?
- How can cyberattacks be prevented?
- What regulations could be put into place to prevent the unnecessary and dangerous growth of nuclear weapons programmes?

Useful links:

<https://nuclearnetwork.csis.org/cyber-nuclear-nexus-how-uncertainty-threatens-deterrence/>

<https://time.com/5922897/us-nuclear-weapons-energy-hacked/>

<https://www.nti.org/analysis/articles/cyber/>

<https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf>

<https://www.theguardian.com/world/2024/feb/08/cyber-attacks-by-north-korea-raked-in-3bn-to-build-nuclear-weapons-un-monitors-suspect>