Imminent Cyber Crisis: The Intangible Threat of Quantum Computing

By. Cynthia S.R. Sipahutar

Cyberspace is an essential, intricate, and crucial domain for modern civilization (Berg and Kuipers, 2022). The computer system was built decades ago and has been advancing more swiftly than the top speed of an aircraft. The cornerstone of science and technology studies posits that humanity's need for science and technology will perpetually remain insatiable. Ray Kurzweil declared that technology's speed and capabilities would exceed those of the brain. As a result, the singularity will approach a point where machines will enable people to transcend their brains (Kurzweil, 2005). What are the implications for technology security risks inside the cyber domain? As technology advances, cyberspace has emerged as an ideal arena for new forms of harm, whose methods and goals remain unidentified. Furthermore, actors become more resistant to legal attribution as a result of a new phenomenon in cyberspace known as implausible deniability.

Cyber crises are primarily triggered by the ability of attacks to occur remotely and simultaneously across several places. Furthermore, the most challenging aspect of managing a cyber crisis is the difficulty in identifying the perpetrators responsible for the global attack. Insufficient leadership, minimal risk awareness, and inadequate technology management abilities are important factors jeopardizing infrastructure enterprises and organizations. States and non-state entities predominantly depend on the daily operation of critical infrastructures that have already adopted digital transformation and automated manufacturing, including power plants, oil and gas facilities, railway systems, hospitals, and banking institutions. Many of these emerging technological enterprises were expanding in response to the rising demand for market share and global trade competitiveness.

The SolarWinds attack that hit the United States in 2020 was an unprecedented incident, especially for a technologically advanced nation. It shows that the cyber-induced crises undermine state sovereignty and immunity from any malicious cyber-attacks, notwithstanding their supremacy ICT infrastructures. The attack on software supply chain effectively manipulated government and private companies, with 18,000 clients and 37 defense firms reporting breaches to the Pentagon including Microsoft, Intel, and US Homeland Security. It undoubtedly incapacitated US national security, as the majority of the nation was heavily dependent on computer network services.

Imagine if we were to encounter a similar attack today, but instead of focusing on software, it would target encrypted data and information that was accessible to all individuals worldwide, without regard for their background, race, religion, or profession, only on the count of qubits. The emergence of quantum technology in computer networks significantly jeopardizes personal and confidential data more severely than in SolarWinds case. Quantum computing offers unprecedented acceleration in the capacity of computers to execute various tasks. This domain of computer science employs quantum theory, which elucidates the behavior of energy and matter at atomic and subatomic scales. Despite their sophistication and advancements in valuable discoveries and technologies, powerful quantum computers may create new hacking probabilities by breaching “unbreakable” encryption within minutes.

The South China Morning Post (SCMP) recently reported that Chinese researchers, led by Weng Chao from Shanghai University, announced their debut quantum attack utilizing Canada’s D-Wave system to compromise cryptographic methods, signifying a notable advancement in Chinese cybersecurity capabilities. The system targeted the foundational structure of the Advanced Encryption Standard (AES), specifically the Present, Gift-64, and Rectangle algorithms, which are key representatives of the Substitution-Permutation Network (SPN) and are recognized as the standard for military specifications and the most secure encryption standard. The current development presents imminent crises for both military and civilian infrastructures if stakeholders fail to respond proactively and promptly. If quantum-enabled SolarWinds attacks recur, security and economic stability would be deteriorating, and critical infrastructure may experience significant damage.

We are on the verge of a quantum revolution as the quantum era in cyberspace approaches. It also implicates the dynamic environment in international politics and global security. Quantum computing in cyberspace can bolster the 'cyber arms race' as big powers such as the United States and China develop indigenous quantum computing technology and infrastructures, including for military purposes. Currently, the US government is building cyber resilience against quantum computing assaults through international alliances involving both the public and private sectors around the world. Under the Quantum Security Preparedness Act 2021, the United States implemented confidence-building measures (CMB) initiatives with third-party governments to reduce the possibility of breaches from adversaries such as China and Russia.

The urgency for stakeholders to promptly adjust to emerging cybersecurity standards and monitor regulatory changes will be crucial in readiness for quantum cyber-attacks. The US National Institute of Standards and Technology (NIST) recently published the initial set of Post-Quantum Encryption Standards that was initiated in 2016. The 8-year effort guidelines encompass the encryption algorithm's code, usage instructions, and its purposes. NIST establishes two backup standards in the event of assaults on the three algorithms outlined

in these standards. Countries such as Canada that meticulously adhere to these security norms can anticipate greater resilience against quantum attacks. The fundamental benefit is sustained economic agility resulting from any form of technological disruption, including quantum computing. Thereby, states are encouraged to implement preemptive strategies in the Cyber Quantum era to mitigate more catastrophic occurrences in cyberspace.

Author Short Bio:

Cynthia S.R. Sipahutar is a Lecturer in the Department of International Relations, Faculty of Humanities, Bina Nusantara (BINUS) University. Her main research topics are Security studies and international law. She holds a master's degree in international law from The University of Melbourne, with 8 years of experience practicing in State-owned aircraft manufacturing company.

References

Berg, B. van den, & Kuipers, S. L. (2022). Vulnerabilities and cyberspace: a new kind of crisis. *Oxford Research Encyclopedia Of Politics*. doi:10.1093/acrefore/9780190228637.013.1604

Kurzweil, Ray. (2005) The Singularity is Near: When Human Transcend Biology. *The Viking Press.*