Disarmament and International Security - Research Report II

Addressing the Issue of Cybersecurity Threats to International Security

Introduction to the Topic:

Cybersecurity threats have become an issue in today's interconnected world, bringing many risks to international security. These threats can come in many forms, including hacking, ransomware, disinformation campaigns and attacks on infrastructure like power grids and government systems. Cybersecurity threats undermine global peace and stability, targeting nations, organizations and innocent individuals. As technology advances, the potential for cyberattacks to harm governments, economies and societies grows. Currently, cyberattacks are becoming more frequent and damaging. Examples include large-scale ransomware attacks that ruined healthcare systems and global supply chains, as well as cyberwarfare between nations, where countries target each other's defence or political systems. Cybersecurity threats are a global problem. Nations like the United States, China and Russia are frequently involved in cybersecurity disputes, while countries with less developed cybersecurity infrastructure, such as those in the Global South, are especially vulnerable to attacks.

Causes and Consequences

The rise in cybersecurity threats can be connected to advancements in technology, the spread of digital infrastructure, and weak international regulations. Moreover, groups like cybercriminal organizations, hacktivists, and even state-sponsored hackers exploit these gaps in technological infrastructure.

The consequences of cyberattacks include financial losses, national security breaches, and public safety risks. For example, attacks on healthcare systems can endanger lives, while disinformation campaigns threaten democratic elections.

Include fig. 1.1

fig. 1.1 Verizon Data Breach Investigations Report

Background Information:

Cybersecurity became a significant issue in the early 2000s as the internet grew. Incidents like the 2007 cyberattacks in Estonia. These were a series of cyberattacks targeting the government, banking, and media websites, potentially brought on by the relocation of a soviet war memorial. These attacks disrupted important services, making them one of the first major instances of coordinated state-linked cyberwarfare attacks. Believed to be politically motivated, were early warnings of how cyberattacks could destabilize nations. Vital historical cyberattacks can be seen in figs. 1.2, 1.3, 1.4, all from the *TealTech - Lessons Learned from the Evolution of Cybercrime.* These infographics depict some of the most important cyberattacks over the last 80 years and should be referred to when looking for past examples of cyberattacks.

fig. 1.4 - TealTech - Lessons Learned from the Evolution of Cybercrime

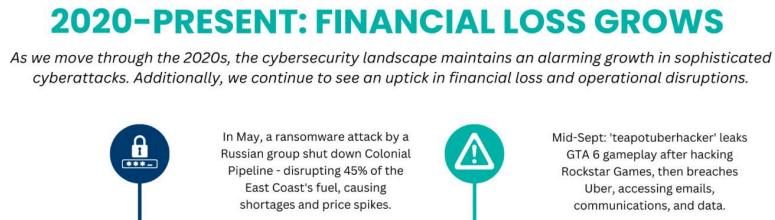

fig. 1.2 - TealTech - Lessons Learned from the Evolution of Cybercrime

fig. 1.3 - TealTech - Lessons Learned from the Evolution of Cybercrime

Recent Developments:

In recent years, governments worldwide have introduced cybersecurity laws and strategies, like the EU's General Data Protection Regulation (GDPR) and the U.S. National Cyber Strategy. Tensions between major powers, like the U.S. accusing Russia and China of state-sponsored cyber-attacks, have increased. Efforts like the United Nations' Group of Governmental Experts (UNGGE) aim to establish norms for responsible behaviour in cyberspace. Emerging technologies, such as artificial intelligence and quantum computing, could either strengthen cybersecurity defenses or make attacks more dangerous. Fig. 1.5 demonstrates the growth in ransomware payments over the last 4 years. *Chainalysis - Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline.*

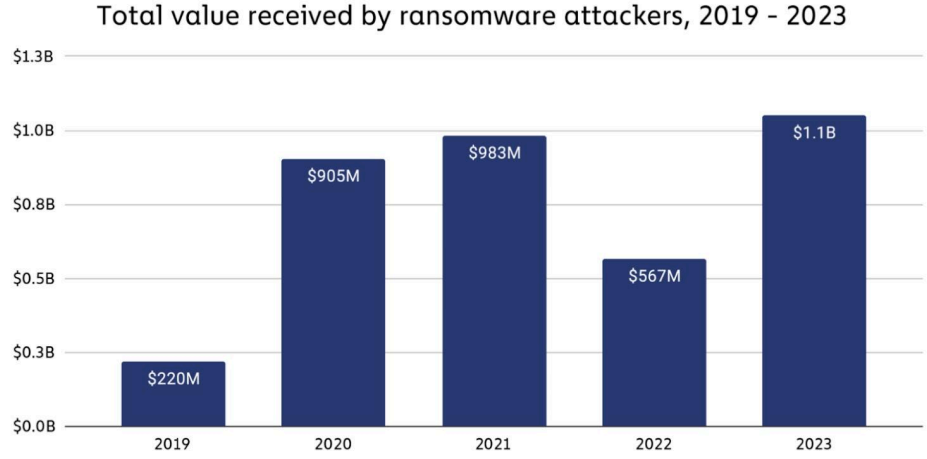

fig. 1.5 - Chainalysis - Ransomware Payments Exceed $1 Billion in 2023, Hitting

Record High After 2022 Decline.

Focus of Debate:

The debate should focus primarily on how to establish international norms and laws to regulate cyberspace and punish cyber criminals. Furthermore, the role of the private sector in securing critical infrastructure and the ability to provide technical and financial support to developing countries to improve their cybersecurity capabilities are vital points for this debate to run smoothly and have reasonable conclusions.

Parties Involved:

United States: Regular target of cyberattacks and an advocate for stronger global cybersecurity regulations. Although they have global leadership in cybersecurity, they seek to establish international norms and frameworks to address cybersecurity threats. Often working with allies to promote responsible behaviour in cyberspace.

Russia and China: Accused of engaging in state-sponsored cyberwarfare, but also victims of cybercrime themselves. Russia supports the creation of a UN-led international legal framework for cybersecurity, but their proposals focus more on restricting the use of cyber tools. China is a global leader in technological developments and cyber capabilities, but they tend to collaborate closely with Russia on cybersecurity policies.

European Union: The EU is a global leader in cybersecurity policy, prioritizing regulation and collaboration. It currently works to standardize cybersecurity across member states, combat cybercrime, and protect critical infrastructure.

Developing Nations: Not only do developing countries lack infrastructure and resources, but they also are targets for cybercrime. This is because cyber criminals have a tendency to target weaker legal systems and under-resourced law enforcements that wouldn't be able to pursue and investigate potential threats.

Tech Companies (e.g., Microsoft, Google): Tech companies, especially those with a focus on hardware, software and cloud sectors, invest heavily in cybersecurity infrastructure to protect their networks, data, and user information. They also collaborate with law enforcement to share threat intelligence, reporting breaches, and supporting investigations into cybercrimes such as hacking, phishing, and identity theft.

Glossary and Key Terms:

Hacking - Unauthorized access to or manipulation of computer systems, network or data.

Disinformation Campaigns - Coordinated efforts to spread false or misleading information, often to manipulate public opinion or disrupt social and political processes.

State-Sponsored Hackers - Hackers or groups supported by governments to carry out cyber operations, often targeting other nations' security or interests.

Artificial Intelligence - The use of machines and algorithms to simulate human intelligence, which can strengthen cybersecurity defenses or be exploited for cyberattacks.

Quantum Computing - Advanced computing technology that uses quantum mechanics, with potential to revolutionize encryption and cybersecurity.

GDPR (General Data Protection Regulation) - A legal framework enacted by the European Union to protect individuals' privacy and personal data in the digital space.

UNGGE (United Nations Group of Governmental Experts) - A UN-led initiative to create norms and guidelines for responsible behaviour in cyberspace.

APTs (Advanced Persistent Threats) - Long-term cyber campaigns conducted by well-funded and organized actors, often targeting sensitive or strategic systems.

Global South - A term used to describe developing nations, often more vulnerable to cyberattacks due to weaker cybersecurity infrastructure.

Possible Solutions:

- A UN-regulated cybersecurity research council that ensures ethical practices in the development of cyber tools and prevent the misuse of research for malicious purposes that mandates transparency in the development of offensive cyber tools and supports research into defense mechanisms against advanced persistent threats (APTs).
    - Establishing a UN Cyber Peacekeeping Force that is composed of technical experts from member states that respond to major cyber incidents and has the ability to mediate between nations in the event of cyber conflicts.
    - The implementation and development of a UN-led international legal framework for prosecuting cross-border cybercrimes, ensuring fair and consistent regulations such as the facilitation of cooperation between law enforcement agencies of member states to investigate and prosecute cyber criminals.

Past UN Actions:

- The UN has established frameworks like the UNGGE to discuss state behavior in cyberspace. The Sustainable Development Goal (SDG) 16 emphasizes peace, justice, and strong institutions, which relate to cybersecurity.

- UN Resolution 73/27 on the Advancement of Responsible State Behaviour in Cyberspace (2018) was a resolution that emphasized the need for cooperation to ensure the security of information and communication technologies. It also promoted the idea that international law, including the UN Charter, applies to cyber activities.

- The UN's Internet Governance Forum (IGF) was launched in 2006 and provides a platform for multi-stakeholder dialogue on internet governance, cybersecurity, and the fight against cybercrime. It collects governments, the private sector, civil society, and technological communities to discuss various aspects of cybersecurity policy.

- UN Resolution 74/247 on Combating Cybercrime (2019) was aimed at strengthening international cooperation in addressing cybercrime and enhancing cybersecurity. It called for increased sharing of information and collaboration between nations to tackle cybercrime.

Bibliography and Useful Links:

1. Chainalysis Ransomware Report: https://blog.chainalysis.com/reports/

2. Cybersecurity Ventures - Timeline of Attacks: https://cybersecurityventures.com/

3. TealTech - https://tealtech.com/blog/cyber-attack-history/

4. United Nations Office for Disarmament Affairs: https://www.un.org/disarmament/topics/information-security/

5. Verizon Data Breach Investigations Report: https://www.verizon.com/business/resources/reports/ dbir/

6. World Economic Forum - Global Risks Report 2023: https://www.weforum.org/reports/the-global-risks- report-2023/