Forum: GA1 Disarmament and International Security Committee

Issue: Developments in the Field of Information and Telecommunications in the Context of International Security (402)

Student Officer: Kelly Hu

Introduction

In an era marked by rapid technological advancements, the role of information and telecommunications has become paramount in shaping global security dynamics. Modern telecommunications and information technologies offer tremendous opportunities for socio-economic development, international collaboration, and technological innovation. However, they also present significant challenges, including cybercrime, data breaches, misinformation, and cyberwarfare. The dual-use nature of these technologies—capable of promoting progress and inflicting harm—has raised pressing questions about their governance, ethical use, and role in maintaining international peace and security.

This issue is particularly emphasized by Sustainable Development Goal (SDG) 16, which promotes peace, justice, and strong institutions. SDG 16 aims to foster peaceful and inclusive societies, ensure access to justice for all, and build effective, accountable, and inclusive institutions at all levels. It underscores the importance of reducing violence, combating organized crime, and addressing corruption and bribery. In the context of information and telecommunications, SDG 16 highlights the need for resilient systems that can counter cybercrime, misinformation, and malicious digital activities such as ransomware attacks, intellectual property theft, and the manipulation of information to destabilize governments. The goal also emphasizes public access to information and the protection of fundamental freedoms, advocating for global cooperation to create secure technological ecosystems that uphold transparency and accountability. These efforts are essential to address the vulnerabilities that threaten sovereignty, stability, and safety, and to ensure that technological advancements contribute to international peace and equitable development.

As nations increasingly rely on interconnected systems for communication, infrastructure, and defense, ensuring the security of information and telecommunications technologies has become critical. The issue calls for a comprehensive, cooperative approach to address threats while fostering innovation and accessibility for all.

Definition of Key Terms

Information and Telecommunications Technologies (ICTs) -

The diverse range of technologies used to transmit, receive, and store information. This includes the internet, telecommunication networks, satellites, and emerging technologies such as artificial intelligence and blockchain.

Cybersecurity -

The practice of protecting computer systems, networks, and data from cyber threats, such as hacking, data breaches, and malware attacks. In the context of international security, cybersecurity measures are critical to preventing cyber warfare and safeguarding national infrastructure. Countries and international organizations, like the United Nations Group of Governmental Experts (UNGGE), debate norma and frameworks for responsible state behavior in cyber space.

Cybercrime -

Illegal activities conducted through or targeting information and telecommunications technologies. Examples include hacking, identity theft, and cyber fraud.

Cyberwarfare -

The use of cyberattacks by a nation-state to disrupt or damage the operations, infrastructure, or security of another state. These activities can include sabotage, espionage, or the spread of disinformation.

Critical Infrastructure -

Systems and assets that are vital to a nation's security, economy, and public health. These include energy grids, transportation networks, water supply systems, and communication networks.

Ransomware attack -

A type of cyberattack in which malicious software encrypts a victim's data or locks them out of their systems, demanding a ransom payment—typically in cryptocurrency—in exchange for restoring access. These attacks often target businesses, institutions, or individuals, causing significant financial losses and disruptions to critical operations if ransom is not paid.

Intellectual property theft -

Intellectual property theft involves the unauthorized use, reproduction, or distribution of someone else's intellectual property, such as patents, copyrights, trademarks, or trade secrets, without permission or legal rights. This theft undermines innovation, causes financial losses to creators or companies, and often results in legal disputes or competitive disadvantages in industries reliant on proprietary information.

Information Warfare -

The strategic use of misinformation, propaganda, or cyber operations to manipulate public opinion, disrupt political stability, or gain a competitive advantage. Disinformation campaigns, often spread through social media and state-sponsored actors, can influence elections, fuel conflicts, and weaken trust in institutions. Nations debate regulations on information warfare regulations on information warfare while balancing concerns over freedom of speech and national security.

Critical Infrastructure Protection (CIP) -

Measures taken to secure essential sectors like energy, healthcare, transportation, and finance from cyber threats and attacks. The Tallinn Manual on International Law Applicable to Cyber Warfare provides guidance on how international law applies to cyberattacks on critical infrastructure. Governments and private sector entities collaborate to enhance resilience against cyber threats, recognizing cyber security as a key aspect of national security.

Digital Sovereignty -

The ability of a state to govern and regulate digital activities within its borders, including data control, cybersecurity policies, and the regulation of foreign tech companies. Countries like China and Russia advocate for strict internet governance, while others, such as the United States and European Union, promote an open and global internet. The debate over digital sovereignty involves balancing national security , human rights, and economic innovation.

Background Information

Origins of the Issue -

The proliferation of telecommunications technologies dates back to the 20th century, with the advent of telegraphs, telephones, and satellites. As these technologies evolved, they became central to the functioning of societies, economies, and governments. By the 21st century, the internet and digital communication platforms emerged as transformative forces, revolutionizing the global exchange of information.

However, this rapid technological progress also introduced new threats. The 1980s witnessed some of the first instances of cybercrime, while the early 2000s saw an explosion in cyberattacks targeting critical infrastructure, businesses, and individuals. The digital transformation of industries and the rise of social media further exacerbated vulnerabilities, leading to concerns about privacy, misinformation, and the weaponization of technology. Below are some of the current challenges awaiting resolution:

Cybercrime and Cybersecurity Threats -

Ransomware attacks and data breaches have grown in scale and sophistication, targeting governments, corporations, and individuals. According to INTERPOL, global losses due to cybercrime are expected to exceed $10 trillion annually by 2025.

Misinformation and Propaganda -

The dissemination of fake news and the use of social media to manipulate public opinion have threatened democratic processes and international relations. Notably, incidents of election interference through digital platforms have highlighted the need for robust digital safeguards.

Emerging Technologies -

The rapid deployment of artificial intelligence (AI), quantum computing, and 5G networks has introduced both opportunities and risks. While these technologies promise significant advancements, they also create new attack surfaces and ethical dilemmas.

Lack of International Regulations -

Despite the global nature of cyberspace, international norms and treaties governing its use remain underdeveloped. Disagreements on sovereignty, data privacy, and the right to regulate cyberspace hinder collective action.

Key Issues

Cybersecurity Governance -

The lack of a unified framework for addressing cybersecurity has led to fragmented responses to global cyber threats. Building consensus among nations with varying priorities remains a challenge.

Protection of Critical Infrastructure -

Cyberattacks targeting energy grids, healthcare systems, and transportation networks pose significant risks to national security and public safety.

Digital Divide -

Inequities in access to secure and reliable information technologies exacerbate global disparities, leaving vulnerable nations more exposed to cyber threats.

International Cooperation -

The transnational nature of cyber threats necessitates cooperation, yet geopolitical rivalries and mistrust often undermine collaborative efforts.

Major Parties Involved

The United States of America -

The U.S. is a leader in technology innovation and cybersecurity policy, heavily influencing international discourse on information and telecommunications security. It has developed advanced cyber defense and offense capabilities, with agencies like the Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA) leading efforts to secure critical infrastructure and prevent cyberattacks. The U.S. advocates for open internet governance and international cooperation to combat cybercrime, but it also prioritizes national security through measures such as export restrictions on sensitive technologies like semiconductors and artificial intelligence. U.S.-based tech companies like Google, Microsoft, and Amazon also play a central role in shaping global ICT standards.

China -

China is a major player in ICT development and cyber operations, with significant investments in 5G, AI technologies, and quantum computing, spearheaded by companies like Huawei, Tencent, and Alibaba. The country adopts a cyber sovereignty approach, asserting that each nation should have the right to control its own cyberspace, including content regulation and data localization. China's policies on internet governance often diverge from Western norms, focusing on state control rather than open access. Accusations of state-sponsored cyber activities, such as intellectual property theft and espionage, have heightened tensions with other nations. Despite Criticism, China continues to promote its Digital Silk Road initiative, aiming to establish global influence by exporting its ICT infrastructure and governance models.

Russia -

Russia is frequently accused of state-sponsored cyber activities, including election interference, cyber espionage, and ransomware operations attributed to groups like Fancy Bear and Cozy Bear. It advocates for a government-controlled internet, often opposing western calls for an open and collaborative

cyberspace. Russia has also proposed international agreements, such as a UN cybersecurity treaty, that align with its stance on cyber sovereignty. Despite accusations of undermining international security, Russia maintains that its cyber operations are defensive and aimed at ensuring national security. It has repeatedly rejected participation in frameworks like the Budapest Convention on Cybercrime, arguing that they are Western-centric.

European Union -

The EU emphasizes data privacy, cybersecurity, and setting global standards through comprehensive frameworks. The General Data Protection Regulation is one of the most stringent data privacy laws globally, influencing policies beyond Europe. The EU cybersecurity act, implemented in 2019, aims to strengthen the cybersecurity capabilities of member states, create certification schemes for ICT products, and promote cooperation. The EU also funds research and development to counter cyber threats and mitigate risks associated with emerging technologies. Despite its strong frameworks, the EU faces challenges in ensuring uniform implementation across member states and addressing external threats.

International Telecommunication Union (ITU) -

The ITU, a specialized agency of the United Nations, facilitates international cooperation on ICT issues. It plays a key role in fostering dialogue on global cybersecurity, digital inclusion, and the ethical use of emerging technologies. The ITU's World Summit on the Information Society (WSIS) aims to bridge the digital divide and establish a secure and inclusive global information society. However, the ITU faces criticism for its slow decision-making processes and challenges in aligning the priorities of member states with divergent views on cyber governance.

Evaluation of Previous Attempts to Resolve the Issue

Budapest Convention on Cybercrime (2001) -

The Budapest Convention was the first international treaty designed to address cybercrime by providing legal frameworks for investigating, prosecuting, and cooperating across borders. It covers offenses like

unauthorized access, data interference, and computer-related fraud, aiming to harmonize national laws and improve international collaboration. However, its effectiveness is limited due to the non-participation of key nations such as Russia and China, which argue that the treaty reflects Western priorities. These non-signatory states have instead advocated for alternative frameworks under the UN that emphasize national sovereignty.

United Nations Group of Governmental Experts (UNGGE) -

The UNGGE was established to develop norms of responsible state behavior in cyberspace and promote transparency and confidence-building measures. While the groups succeeded in facilitating dialogue and producing voluntary norms, such as refraining from cyberattacks on critical infrastructure, it failed to achieve binding agreements. Geopolitical divisions, particularly between Western nations and states like Russia and China, prevented consensus on key issues like attribution of cyberattacks and accountability mechanisms. Despite its shortcomings, the UNGGE remains a platform for dialogue and has informed subsequent efforts to develop cyber norms.

Paris Call for Trust and Security in Cyberspace (2018) -

The Paris Call, initiated by France, is a multilateral initiative endorsed by over 70 countries, along with private sector companies and civil society organizations. It advocates for principles such as protecting critical infrastructure, ensuring electoral integrity, and addressing cybercrime. While it demonstrates broad support, the initiative lacks enforcement mechanisms, reducing its practical impact. Key nations like the United States, Russia, and China have not endorsed the Paris Call, limiting its ability to achieve global consensus. Nonetheless, it represents an important step toward fostering multi-stakeholder collaboration on cyber security.

Possible Solutions

Developing a Global Cybersecurity Framework -

Establishing binding international treaties to govern cyber activities, protect critical infrastructure, and promote responsible state behavior in cyberspace.

Enhancing Cybersecurity Capacity in Developing Nations -

Providing technical assistance, funding, and training to bridge the digital divide and improve the resilience of vulnerable nations against cyber threats.

Promoting Public-Private Partnerships -

Encouraging collaboration between governments, technology companies, and civil society to develop innovative cybersecurity solutions and address global threats.

Strengthening Cyber Norms and Accountability -

Building consensus on norms for responsible state behavior in cyberspace and establishing mechanisms for transparency and accountability.

Investing in Emerging Technology Ethics -

Developing guidelines for the ethical use of AI, quantum computing, and other emerging technologies to ensure they are harnessed for positive purposes.

Relevant UN Resolutions and Frameworks

Resolution 73/27 (2018): Developments in the Field of Information and Telecommunications in the Context of International Security.

Resolution 74/29 (2019): Advancing Responsible State Behavior in Cyberspace.
Sustainable Development Goal 16 (2015): Promote Peace, Justice, and Strong Institutions.

Bibliography

[1] “Budapest Convention - Cybercrime - Www.Coe.Int.” *Cybercrime*, 8 Feb. 2024, www.coe.int/en/web/cybercrime/the-budapest-convention. Accessed 25 Jan. 2025.

[2] “Financial and Cybercrimes Top Global Police Concerns, Says New Interpol Report.” *INTERPOL*, www.interpol.int/en/News-and-Events/News/2022/Financial-and-cybercrimes-top-global-police-concerns-says-new-INTERPOL-report. Accessed 25 Jan. 2025.

[3] “Why We Need Global Rules to Crack down on Cybercrime.” *World Economic Forum*, www.weforum.org/stories/2023/01/global-rules-crack-down-cybercrime/. Accessed 25 Jan. 2025.

[4] *Visa Prevented $40 Bln Worth of Fraudulent Transactions in 2023- Official | Reuters*, www.reuters.com/technology/cybersecurity/visa-prevented-40-bln-worth-fraudulent-transactions-2023-official-2024-07-23/. Accessed 25 Jan. 2025.

[5] Banchereau, Mark. “Interpol Clamps down on Cybercrime and Arrests over 1,000 Suspects in Africa.” *AP News*, 26 Nov. 2024, apnews.com/article/208111329edd3a1a64faf85cc7c0d2c0. Accessed 25 Jan. 2025.

[6] “The Role of UNODC in Cybercrime Prevention.” *United Nations : Office on Drugs and Crime*, www.unodc.org/unodc/en/cybercrime/. Accessed 25 Jan. 2025.

[7] “Cybersecurity Framework.” *NIST*, 14 Jan. 2025, www.nist.gov/cyberframework. Accessed 25 Jan. 2025.

[8] *OECD Digital Education Outlook 2023 | OECD*, www.oecd.org/en/publications/oecd-digital-education-outlook-2023_c74f03de-en.html. Accessed 25 Jan. 2025.

[9] “Global Cybersecurity Index.” *ITU*, www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx. Accessed 25 Jan. 2025.

[10] “Resolution 73/27: Developments in the Field of Information and Telecommunications in the Context of International Security.” *United Nations*, digitallibrary.un.org/record/1660706. Accessed 25 Jan. 2025.

[11] “Cybercrime.” *INTERPOL*, www.interpol.int/en/Crimes/Cybercrime. Accessed 25 Jan. 2025.

[12]“The Economic Impact of Cybercrime.” *404 Error - Page Not Found*, www.worldbank.org/en/news/feature/2023/07/15/the-economic-impact-of-cybercrime. Accessed 25 Jan. 2025.

[13]“Cybersecurity and International Relations.” *The Belfer Center for Science and International Affairs*, 1 June 2024, www.belfercenter.org/topics/science-technology/cyber-security. Accessed 25 Jan. 2025.

[14] “Cyber Threat Report 2023.” *NCSC.GOVT.NZ*, www.ncsc.govt.nz/resources/ncsc-annual-cyber-threat-reports/2023-web. Accessed 25 Jan. 2025.