

BSAMUN 2024

NATO

Developing A Secure Cyberspace For All Users

President Chair: Kira Tarasova

Deputy Chair: Lara Waatjes

Introduction

In today's interconnected world, cyberspace serves as a fundamental component in facilitating communication, commerce, and collaboration on an unprecedented scale. Digital infrastructure is increasingly the backbone of prosperous militaries, transparent governments, and free societies. As never before, information technology fosters transnational dialogue and facilitates the global flow of goods and services. These social and trade links have become indispensable to our daily lives. Social and political movements rely on the Internet to enable new and more expansive forms of organisation and action. The reach of networked technology is pervasive and global. This makes cyber diplomacy essential as it can preserve state secret information, national infrastructure and identities whilst preventing cyber attacks on nations.

As international political tensions arise, nations need to work together to prevent cyber attacks on privacy, human rights, economic stability, and national security, by considering the global interconnectedness of the digital ecosystem. State and non-state actors alike have exploited vulnerabilities in digital infrastructure to launch cyberattacks aimed at disrupting critical systems, stealing sensitive information, and undermining the integrity of democratic institutions. The proliferation of cyber threats has fueled tensions among nations, leading to an escalation of cyber-enabled conflicts and raising concerns about the erosion of trust and stability in the international system. The future of cyberspace remains vague and unexpected, but it is certain to have far-reaching repercussions on many aspects of human existence as digital technologies have facilitated unprecedented levels of connectivity and engagement, enabling governments to enhance diplomatic relations, foster economic integration, and address transnational issues.

Key Terms

Cyberspace: Space in which users share information, and interact with each other; engage in discussions or social media platforms

Cyberwarfare: A series of cyber attacks against a nation-state, causing it significant harm



Cybercrime: Any criminal activity that involves a computer, network or networked device.

UN Office of Counter-Terrorism (UNOCOT): Helps countries work together to stop terrorists from using the internet and digital tools to plan and carry out attacks. They do this by creating rules, helping countries build skills and sharing information.

NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE): Is a NATO-accredited international military organisation that focuses on a range of aspects related to cybersecurity.

Group of Governmental Experts (GGE): Developed the norms of responsible state behaviour in cyberspace- enforces the international law, state sovereignty and human rights that apply to cyberspace.


UN Programme of Cyber Action: Aims to promote peace, security, and stability in cyberspace through a cooperative model that advances the exchange of knowledge and practices, avoids duplication of efforts and assists in national and regional implementation efforts

General Overview

In an era where technology infuses every aspect of one's life, the issue of cybersecurity has stood at the forefront of global concern since the introduction of cyberspace in 1987. It has facilitated global connectivity, collaboration and personal and professional relationships. The interconnected nature of our digital world has brought unparalleled opportunities for communication and cloud services. However, it has also exposed many risks, from data breaches to cyber-attacks that threaten the fabric of our societies, posing challenges like information overload, privacy breaches, cyberwarfare and cyberterrorism.

Cyberwarfare

As the strategic importance of cyberspace continues to grow, member states must adapt to the evolving threat, developing innovative strategies and capabilities to defend against emerging cyber threats and safeguard national interests in an increasingly interconnected world. State-sponsored cyber attacks often involve the use of tools and techniques developed by intelligence agencies and military units to achieve strategic objectives, such as espionage and sabotage. Non-state actors, on the other hand, exploit



cyberspace to advance ideological agendas, promote social or political causes, or pursue financial gain through cybercrime activities. As a result, the traditional notions of territorial sovereignty and jurisdiction are challenged, requiring collaborative efforts among nations to address the transnational nature of cyber threats effectively. These attacks can target critical infrastructure and can have far-reaching consequences, disrupting services, undermining public trust, and inflicting economic and social costs, resulting in billions of dollars in losses each year.

Cybercrime

Cyberspace enables cybercriminals to operate on a global scale with relative anonymity. This transcends geographical boundaries and enables adversaries to target victims anywhere in the world. Cyberattacks can be launched from remote locations, crossing international borders with ease and anonymity. This global reach makes it challenging for law enforcement agencies to track down cybercriminals, as they often operate from jurisdictions with moderate cybercrime laws or limited enforcement capabilities. Advances in technology have expanded the arsenal of cybercriminals, enabling the development of increasingly sophisticated malware, ransomware, and hacking tools. The proliferation of underground forums and dark web marketplaces has lowered the barriers to entry for aspiring cybercriminals, allowing them to access tools and expertise previously available only to seasoned hackers. Moreover, artificial intelligence and cryptocurrencies have introduced new challenges for law enforcement agencies, enabling cybercriminals to evade detection and launder illicit procedures more effectively.

The UN's participation in cyberspace started in 2019 when the UN developed a GGE. They have been preventing cyber conflicts and promoting international cooperation by increasing member states' confidence to enhance their transparency in cyberspace. Additionally, the UN Programme of Cyber Action continuation of previous consensus work in the GGEs and Open-ended Working Groups (OEWGs) to consider, implement and advance responsible State behaviour in cyberspace and further build upon this work. To the present day, this programme has taken proactive steps to protect governments and businesses to protect themselves in cyberspace by increasing states' cybersecurity capacity.

Currently, any State can be the target of a cyber attack. Some of the most common targets include the United States, South Korea, Japan, Russia, China and the United


Kingdom. Some nations that are best prepared to deal with cyber attacks include, but are not limited to: Canada, the United States, Brazil and Germany. Most of these attacks are suspected from China, Russia, Iran and North Korea.

Major Parties/Countries Involved

United States: The US prioritises information collecting, cybersecurity, and countering cyber threats. Protecting national interests online is a critical function of government organisations like Cyber Command and the National Security Agency (NSA). Furthermore, the FBI and the Secret Service are only two of the law enforcement organisations in the US that are actively fighting cybercrime. To combat global cyber threats, they work with foreign partners to investigate and prosecute a variety of cyber offences. Furthermore, the goal of cybersecurity initiatives and legislative actions is to fortify the nation's defences against cybercrime. With agencies like the United States Cyber Command (USCYBERCOM) spearheading efforts to protect national interests and carry out cyber operations, the US is heavily involved in cyberwarfare as there are persistent cyber threats from North Korea, Iran and transnational criminal organisations.

People's Republic of China: The People's Republic of China is heavily involved in cyberspace both in terms of strategic initiatives and technology developments. The nation places a high priority on cyber capabilities and its military includes a force specialised in cyber warfare. Allegedly supported by the Chinese government, these hackers have been charged with a range of cybercrimes, such as cyber-espionage and theft of intellectual property. Additionally, the government uses monitoring and censorship to maintain control over internet access within the nation. China has been accused of providing sanctuary to cybercriminals and being linked to multiple cyberattacks, but has denied accusations of cyberwarfare, and has accused the United States of engaging in cyber-warfare against it. It is difficult to assign responsibility for cybercrimes to a particular country, hence international collaboration is crucial to combating and preventing these kinds of actions.

United Kingdom: The UK is a major player in cyberspace, with an emphasis on intelligence capabilities, cybersecurity, and national defence. The National Cyber Security Centre (NCSC), offers advice to the public and businesses and is crucial in defending the nation against cyberattacks. The UK possesses offensive cyber capabilities as well, and



the military conducts cyber operations to protect national interests through entities like the Government Communications Headquarters (GCHQ). With the help of law enforcement organisations like the National Crime Agency (NCA) and the Cyber Crime Unit, the UK is actively fighting cybercrime. These organisations look into and punish a variety of cyber offences, including identity theft, hacking, and online fraud. The government of the United Kingdom endeavours to enhance cybersecurity protocols, enact laws, and cooperate with global associates to confront the dynamic terrain of cyber hazards. To safeguard its interests in national security, the UK is heavily involved in cyber warfare, using both offensive and defensive cyber capabilities.

France: France is a prominent participant in cyberspace, emphasising technological developments, cybersecurity, and national defence. To defend vital information systems and fend off cyberattacks, the French government has set up organisations like the National Cybersecurity Agency of France (ANSSI). Cyber capabilities are also incorporated by the military, such as the French Armed Forces, into their defence plan. France has worked to strengthen its national cybersecurity posture in the face of changing cyber threats and participates in international partnerships to solve cybersecurity issues. Through law enforcement organisations like the National Gendarmerie and the Central Office for Combating Cybercrime (OCLCTIC), France actively fights cybercrime. These organisations look into and punish a range of internet crimes, such as identity theft, hacking, and online fraud. To combat the worldwide character of cybercrime, the French government strives to bolster cybersecurity measures, pass legislation, and cooperate with foreign partners. France is dedicated to safeguarding its people and companies from the constantly changing risks associated with the digital sphere. France has integrated cyber capabilities into its national defence plan and is actively engaged in cyberwarfare.

Russian Federation: The Russian Federation is a major participant in cyberspace and is visible in several domains. The nation is renowned for having highly developed cyber capabilities for both offensive and defence purposes. State-sponsored cyber operations, such as influence operations, cyberattacks, and cyber espionage, have been linked to Russia. It has also been accused of providing sanctuary to cybercriminals committing a range of cybercrime. These actions include ransomware assaults, financial fraud, and hacking. Russia's military is heavily involved in these operations, especially its cyber forces. International worry over Russia's intricate engagement in cyberspace has sparked continuing conversations about cybersecurity and appropriate online conduct, although it


can be difficult to assign blame for cybercrimes to a particular country. Russia sees activities in cyberspace as a subset of the all-encompassing framework of 'information confrontation,' which is derived from the Russian understanding of relations between states and, more specifically, a subset of the struggle between great powers for influence in the world. The Russian Ministry of Defence describes the information confrontation as the clash of national interests and ideas, where superiority is sought by targeting the adversary's information infrastructure while protecting its objects from similar influence

NATO: NATO understands the value of cybersecurity in the current threat environment. To improve its capacity to counter cyber threats, the alliance launched a Cyber Operations Centre in 2012. To improve collective cybersecurity defences, NATO member nations work together on information sharing, coordinated exercises, and capacity-building. The alliance has stated that a cyberattack may be grounds for collective defence under Article 5 of the NATO treaty if it is deemed an act of aggression. NATO's main priorities are collective security and defence, which includes protecting member states against cyberattacks. Although it does not actively participate in cybercrime law enforcement, NATO works with its member states to exchange intelligence, carry out cooperative training, and develop capabilities that improve cybersecurity. NATO's approach to combating cybercrime is more defensive and resilient, focusing on group reactions to cyber threats that may jeopardise member state security. Coordination between NATO, member states, and pertinent law enforcement authorities is usually required to combat cybercrime. NATO regularly participates in discussions about cyberwarfare as it relates to collective defence.

UN Involvement & Relevant Resolutions

UN Resolution 55/63, 2001: Prevented the criminal misuse of information technologies. Ensured that law enforcement will cooperate in investigations and prosecutions of international cases of criminal misuse of information technologies should be coordinated among all concerned States.

NATO Summit in Vilnius, 2023: Endorsed a new concept to enhance the contribution of cyber defence to NATO's overall deterrence and defence posture. The concept will further integrate NATO's three cyber defence levels – political, military and technical –



ensuring civil-military cooperation at all times through peacetime, crisis and conflict, as well as engagement with the private sector, as appropriate.

NATO Summit in Wales, 2012: In this policy, cyber defence was recognised as part of NATO's core task of collective defence, which means that a cyber attack could be grounds to invoke Article 5 of NATO's founding treaty. Member states also recognised that international law applies in cyberspace.

NATO Article 5, 1949: If a NATO state is a victim of an armed attack, each and every other member will consider this act of violence as an armed attack against all member states and will take the actions that seem necessary to assist the Ally attacked.

Possible Solutions:

Securing cyberspace is a global challenge that requires collaboration among countries. With this collaboration, countries can address cross-border cyber threats, promote cybersecurity norms and principles, and strengthen global cybersecurity governance frameworks by enhancing cyber defence capabilities and response readiness. This can refrain from countries engaging in or supporting cyber activities that threaten the peace, security, and stability of other states, including cyberattacks targeting critical infrastructure, electoral systems, and diplomatic communications.

Focus on protecting critical infrastructure, securing government systems, and strengthening resilience against cyber threats. Strengthen legal and regulatory frameworks related to cybersecurity, including laws on data protection and privacy rights, following international law and human rights principles.


Building educational programs to increase cybersecurity awareness at all levels of society. These programmes help them understand how to protect themselves and their information online. By being aware of cybersecurity risks and best practices, people can take proactive steps to keep their personal and financial information safe, reducing the likelihood of falling victim to cyberattacks and fraud.

Strengthen the transparency of a country. This includes the sharing of cybersecurity policies, doctrines, and strategies. When countries are more transparent about their cybersecurity policies, it builds trust and reduces the likelihood of misunderstanding or misinterpretation of actions in cyberspace. This transparency can help prevent the

escalation of conflicts and foster greater cooperation in addressing cyber threats collaboratively. Additionally, transparent communication can lead to better coordination of efforts to prevent cyberattacks, share threat intelligence, and develop norms of responsible behaviour in cyberspace.

Bibliography

- Nato. “Cyber Defence.” NATO, January 17, 2024.
https://www.nato.int/cps/en/natohq/topics_78170.htm
- “Department of Defense Strategy Operating in Cyberspace.” America: Department of Defense, July 2011.
<https://csrc.nist.gov/csrc/media/projects/ispab/documents/dod-strategy-for-operating-in-cyberspace.pdf>
- “Cybersecurity and New Technologies | Office of Counter-Terrorism.” United Nations. Accessed March 4, 2024.
<https://www.un.org/counterterrorism/cybersecurity>
- “The UN and Cyberspace Governance.” orfonline.org. Accessed March 4, 2024
<https://www.orfonline.org/research/the-un-and-cyberspace-governance>
- “Towards Cyberpeace: Managing Cyberwar through International Cooperation.” United Nations. Accessed March 4, 2024.
<https://www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation>
- What is the UN Cybercrime Treaty and why does it matter? | chatham ... Accessed March 4, 2024.
<https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter#:~:text=Since%20May%202021%2C%20UN%20member,instrument%20on%20a%20cyber%20issue>
- “Russia’s Strategy in Cyberspace.” NATO Strategic Communications Centre of Excellence,
https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf

- 
- CyberPeace Institute. “Statement on the Cyber Programme of Action.”

CyberPeace Institute, July 12, 2023.

<https://cyberpeaceinstitute.org/news/statement-cyber-programme-of-action/#:~:text=The%20Cyber%20PoA%20aims%20to,national%20and%20regional%20implementation%20efforts.>

