KEPİRMUN'26
DISEC

Agenda* Item*: Addressing Emerging Threats in Cybersecurity and International Stability

TABLE OF CONTENTS

Letter From Head of Academy

Dear Delegates

It gives me great pride to introduce and welcome you to the DISEC Committee of KEPİRMUN'26. As a team, we are honored to see you take part in this conference as we gather to discuss the highly consequential and newsworthy topic of Cyber Warfare.

Cyber warfare challenges traditional definitions of conflict and battle. Today, war is no longer confined on land, air or sea alone but is also upfront behind computer screens and lines of code. In this committee, you will get a chance to consider the increasing threats emerging from rapidly developing technologies and develop solutions that could be notable for our future one day.

As delegates, you should research extensively, think strategically and represent your country's ideologies professionally. I encourage you to approach this committee with confidence, preparation, and respect for different opinions as you debate to find effective solutions for the challenges ahead.

I trust this conference will be an equally inspiring and meaningful experience for you. Please do not hesitate to contact me or our team in case you have any questions or require assistance.

Yours Faithfully,

Duygu SEZER

Head of Academy

E-Mail: duygusezerkepir5099@gmail.com

Letter From the Under Secretary General of DISEC

Distinguished Delegates,

I'm super glad to welcome you all to the DISEC committee. Our delegates will face on the issues that has arisen due to CyberWarfare ,a global issue that stems from the huge impact of cybersecurity in our daily lives.

Under the framework of the United Nations and the principles established by the Convention Relating to Cybersecurity, we will try to find an agreed upon solution that still stays in the bound of reality. However, the implementation of these principles often presents complex legal and political challenges. The states will have to find a workaround these challenges while still maintaining an agreement within each other.

Throughout the conference, delegates are expected to analyze the importance of Cybersecurity, Cyberattacks and the looming threat of Cyber-warfare with detailed and complex thinking.

As an upper intermediate-level committee, this forum requires extensive knowledge of english and the topic at hand. However you shouldn't be afraid to approach this committee. With some studying you should be more than likely to be successful and have a shot at the prestigious title of 'Best Delegate'.I would recommend you to prepare notes with extensive research of the topic at hand.

I would want to see you sitting in front of me in this committee.

Adar Ege KESEBİR

Under-Secretary-General

E-Mail: a.ege.kesebir@gmail.com

Introduction To The Committee

3) Introduction to the Committee

The Disarmament and International Security Committee (DISEC) is the First Committee of the United Nations General Assembly, responsible for addressing issues related to global security, disarmament, and international peace. The committee focuses on reducing threats that may lead to conflict and aims to promote cooperation among member states in order to maintain international stability.

Within this framework, DISEC examines both traditional and emerging security challenges, including cyber warfare. As technological developments increasingly influence international relations and security, cyber warfare has become a significant issue for the international community. Therefore, DISEC plays an important role in discussing the implications of cyber threats and encouraging states to develop cooperative and effective responses.

3.1 *Overview of DISEC*

The Disarmament and International Security Committee (DISEC) is the First Committee of the United Nations General Assembly and serves as one of the principal forums for addressing issues related to global security and disarmament. Established alongside the structure of the United Nations in 1945, DISEC was created to provide Member States with a platform to discuss threats to international peace and to promote cooperation in limiting and regulating weapons. From its early focus on nuclear disarmament during the Cold War, the committee has gradually expanded its scope to include conventional weapons, arms control, military transparency, and emerging security challenges.

Over time, DISEC has evolved to reflect changes in the global security environment. As technological developments introduced new forms of conflict and security risks, the committee began addressing issues beyond traditional warfare, including outer space security, autonomous weapons systems, and cybersecurity.

3.2 *Powers, Purpose and Functions of DISEC*

DISEC functions as a deliberative body within the United Nations General Assembly, where Member States discuss international security concerns and develop policy recommendations. Although DISEC does not directly enforce policies, it operates by debating agenda items, negotiating draft resolutions, and proposing recommendations that may later be adopted by the General Assembly, thereby guiding international norms and encouraging collective action among states.

3.3 Relevance of Cyber Warfare within DISEC

As digital technologies increasingly influence national security and military operations, cyber warfare has become a significant concern within DISEC's agenda. Cyber attacks targeting government institutions, critical infrastructure, and defense systems have the potential to disrupt societies and escalate international tensions. In this context, DISEC provides an important forum for Member States to discuss the risks posed by cyber threats, promote responsible state behavior in cyberspace, and explore cooperative measures to strengthen cybersecurity. By addressing cyber warfare alongside traditional security issues, the committee contributes to the development of international norms and policies aimed at maintaining stability in the rapidly evolving digital environment.

4) Agenda Item Overview: Cyber Warfare and International Security

The term "Cyber Warfare" is used when states or civilians are damaged by cyberattacks executed by non-state actors and other malicious individuals as such.These cyberattacks damage and limit the states own cyber protections and in doing so hurt the states privacy and infrastructure.The duty of international security is to prevent these cyber threats from inflicting any significant damage to the state and civilians.

5) Historical Background and Current Context

For the current century, multiple cyber incidents and policy responses have shaped international debates on state responsibility, cooperation, and conflict prevention in the digital environment. Over time, cyberspace became a strategic domain that intersected political, economic, and military interests to address this rapidly evolving matter.

5.1 Evolution of Cyber Warfare

The origins of cyber warfare can be traced to the early development of computer networks during the Cold War. As governments began integrating computers into military communication and intelligence systems in the 1960s and 1970s, concerns emerged regarding the vulnerability of digital infrastructure. Early incidents primarily involved espionage rather than direct attacks, such as intelligence agencies exploring methods of accessing adversaries' networks to gather strategic information. Later, with the expansion of the internet in the 1990s, the cyber threat landscape significantly widened and the exploration of networked systems increased across borders.

The early 2000s marked the transition from cyber espionage to politically motivated cyber operations. Large-scale cyber incidents demonstrated that digital attacks could produce national level consequences. Distributed denial-of-service (DDoS) attacks targeting government institutions and financial systems revealed how cyber tools could disrupt public services without conventional military engagement. States increasingly recognized cyberspace as a domain of conflict comparable to land, sea, air, and later space, and creation of national cybersecurity strategies and specialized cyber commands were prompted.

In the 2010s and 2020s, cyber warfare became institutionalized within national defense policies. Many states formally integrated offensive and defensive cyber capabilities into military doctrine, while international organizations began addressing norms of responsible state behavior in cyberspace. However, legal and ethical frameworks have struggled to keep pace with technological developments. Questions surrounding attribution, proportional response, and the applicability of international humanitarian law remain central challenges for policymakers and multilateral forums such as the United Nations.

5.2 *Major Cyber Incidents Affecting International Security*

In 2007, Estonia experienced large-scale distributed denial-of-service (DDoS) attacks targeting government institutions, banks, media outlets, and communication networks. The attacks disrupted essential public services and highlighted how a highly digitalized society could be temporarily destabilized without physical force. This incident prompted international discussions within NATO and the European Union regarding collective cyber defense and resilience.

In 2010, the discovery of the Stuxnet malware marked a significant turning point in cyber warfare. Designed to target industrial control systems, the operation demonstrated that cyber tools could produce physical destruction by sabotaging critical infrastructure. Stuxnet illustrated the emergence of highly sophisticated, state-level cyber capabilities and raised concerns about escalation, attribution, and the legality of cyber operations under international law. It also accelerated global investment in both offensive and defensive cyber programs.

In 2014, a cyberattack against Sony Pictures Entertainment occurred. This incident showed how cyber operations could be used for oppression and political signaling beyond military targets. And other additional interference allegations surrounding electoral processes in multiple countries during the mid-2010s emphasized the role of cyber operations in information warfare, disinformation campaigns, and democratic

disruption. These developments broadened the definition of cyber warfare to include psychological and political dimensions.

In 2017, the WannaCry ransomware outbreak spread rapidly across more than 150 countries, severely affecting healthcare systems, businesses, and government services. Shortly afterward, the NotPetya malware caused extensive economic damage worldwide, disrupting shipping, logistics, and multinational corporations. Unlike earlier incidents limited to specific states, these attacks demonstrated the transnational nature of cyber threats, where malware can unintentionally affect global supply chains and civilian infrastructure far beyond the intended target.

5.3 *Existing International Frameworks and Agreements*

- United Nations Group of Governmental Experts (UN GGE) on ICT Security
- United Nations Open-Ended Working Group (OEWG) on Security of and in the Use of ICTs
- Convention on Cybercrime (Budapest Convention) (2001)
- Second Additional Protocol to the Budapest Convention (2022)
- African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) (2014)
- Shanghai Cooperation Organization Agreement on Cooperation in International Information Security (2009)
- European Union Cybersecurity Strategy
- NIS Directive / NIS2 Directive (EU Network and Information Security Directive)
- NATO Cooperative Cyber Defence Framework
- ASEAN Cybersecurity Cooperation Strategy
- Organization of American States (OAS) Inter-American Cybersecurity Program
- Paris Call for Trust and Security in Cyberspace (2018)

- Global Commission on the Stability of Cyberspace (GCSC) Norm Framework
- Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations
- Global Forum on Cyber Expertise (GFCE)
- CyberPeace Institute

6) Key Issues and Discussion Areas

6.1 *Definition of Cyber Warfare Under International Law*

Under international law, cyber-warfare stands for the use of cyber operations by states or other state sponsored actors to disrupt, damage, or gain unauthorized control over another state's information systems or digital networks in a way that can threaten national security and international stability. The term of Cyber-warfare is not defined specifically in any of universal binding treaties, so its legal interpretation is generally derived from existing frameworks of international law, such as the principles of the United Nations Charter, international humanitarian law (IHL), and other international law governing. Cyber operations may be considered an unlawful use of force or even an armed attack when their scale and effects are comparable to kinetic military actions, such as causing physical destruction, casualties, or significant societal disruption.

6.1.1 *Distinction Between Cybercrime and Cyber Warfare*

Cybercrime and cyber warfare are terms which both of them involve malicious activities conducted through digital technologies. However they differ fundamentally in terms of actors, objectives, and legal frameworks under international law.

Cybercrime generally refers to unlawful acts carried out by individuals or non state groups for financial gain, personal benefit, or ideological motives, and is primarily addressed through domestic criminal law and international partnerships for cybercrime governance.

Meanwhile cyber-warfare involves cyber operations conducted by states or state sponsored actors as a part of broader strategic, military, and geopolitical objectives. Cyber-warfare often targets governmental systems and national security institutions. The legal regulation of cyber warfare is primarily regulated under international law.

6.1.2 Developing a Binding International Cyber Treaty

One of the most important issues in combating cyber warfare is the lack of a comprehensive and enforceable international legal framework; this makes the development of a binding international cyber treaty a critical area of discussion. Currently, existing norms, such as those discussed in the United Nations Group of Governmental Experts, are largely voluntary and lack enforcement mechanisms, which limits their effectiveness in preventing cyber conflicts.

A binding agreement could establish clear definitions of cyber warfare, define state responsibilities, and prohibit malicious activities such as attacks on critical infrastructure, electoral systems, and healthcare networks. However, key challenges include differing national interests, sovereignty concerns, and the difficulty of attributing cyberattacks to specific actors.

Furthermore, disagreements over capabilities and obligations between technologically advanced and developing countries complicate negotiations. Despite these obstacles, a binding agreement could promote accountability, reduce the risks of escalation, and enhance international cooperation, making it a significant step toward global cyber stability.

6.2 *Preventing Escalation in Cyber Conflicts*

In today's interconnected world, cyber conflicts can escalate rapidly if not properly managed. Within the scope of the United Nations General Assembly First Committee (DISEC), preventing escalation is crucial to maintaining international peace and security. States must act responsibly in cyberspace, avoid actions that could be interpreted as hostile, and prioritize dialogue and cooperation. Confidence-building measures, such as communication channels between states and shared norms of behavior, can help reduce misunderstandings and prevent cyber incidents from turning into larger conflicts.

6.2.1 *State Responsibility for Cyber Activities*

States are expected to take responsibility for cyber activities originating within their territory or conducted by actors under their control. This includes preventing cyberattacks, investigating incidents, and cooperating with other states when attacks occur. International law principles, such as sovereignty and non-intervention, are increasingly being applied to cyberspace. Holding states accountable encourages

responsible behavior and helps create a safer and more predictable digital environment.

United States of America: The United States of America (USA) plays a leading role in shaping international discussions and policies on cyber-warfare due to its advanced technological infrastructure and global political influence. The country integrates cyber capabilities into its broader defense and foreign policy framework via institutions like the Department of Defense, the Cybersecurity and Infrastructure Security Agency (CISA), and U.S. Cyber Command.

The USA's main priority is to maintain technological dominance and strategic superiority in cyberspace as the country recognizes cyber capabilities as an essential component of modern military power and geopolitical influence. USA also seeks to preserve a global digital environment largely shaped by Western technological standards and U.S. based technology companies, in order to provide both economic advantage and strategic leverage.

Russia: The Russian Federation plays a significant and influential role in international discussions on cyber-warfare and views cyberspace as a strategic arena to advance state interests. Institutions such as the Ministry of Defence, intelligence services, and specialized cyber units have a significant importance in the country and the primary focus is on developing offensive and defensive cyber capacities. Russia considers information and communication technologies essential and emphasizes the concept of information security, which includes both technical cybersecurity and control over information flows.

Russia advocates for stronger state sovereignty over the internet and promotes legally binding international agreements regulating state behavior in cyberspace. The country has supported initiatives within the United Nations calling for greater governmental control over information space and the prevention of cyber operations that could threaten political stability.

India: The Republic of India has emerged as an increasingly important actor in international discussions on cyber-warfare and cybersecurity and a frequent target of cyber incidents due to its rapid digitalization and strategic geopolitical position. As one of the world’s fastest growing digital economies, India is facing persistent cyber threats which target governmental institutions, financial systems, critical infrastructure, and public services.

Cybersecurity takes place into India's national security and governance framework through the institutions like the Ministry of Electronics and Information Technology

(MeitY), the Indian Computer Emergency Response Team (CERT-In), and the Defence Cyber Agency. India encourages a secure, open, and stable cyberspace alongside advocating respect for state sovereignty and for the responsible use of information and communication technologies at the international field.

Japan: Japan is driven by an advanced technological economy and high dependence on digital infrastructure. The country's growing digital connectivity and preparation for major international events further reinforce the need for strong cybersecurity policies and coordinated national protection measures. Some of Japan's frameworks in this field are National center of Incident readiness and Strategy for Cybersecurity (NISC), the Ministry of Defense, and the Self-Defense Forces' cyber units. These institutions mainly prioritize resilience, rapid incident response, the protection of sensitive technological and industrial data.

Japan's primary priority in cyberspace is to safeguard its advanced technological economy and ensure national resilience against increasingly sophisticated cyber threats, particularly those targeting critical infrastructure and sensitive industrial sectors. Japan seeks to protect intellectual property, secure supply chains, and maintain technological competitiveness especially in the rapidly emerging fields of artificial intelligence and semiconductor production. The country also aims to reduce strategic vulnerabilities stemming from external technological dependence by strengthening domestic capabilities and trusted partnerships.

Israel: Israel preserves an important role in the field of cybersecurity due to its advanced technological ecosystem and longstanding security concerns. Israel's primary objective in cyberspace is to maintain a qualitative technological edge over potential adversaries while ensuring the protection of critical national infrastructure and sensitive data systems. Cyberspace is regarded as a critical domain of national defense in the country and is integrated into Israel's broader military and intelligence strategy. Israel Defense Forces (IDF), with particularly its elite cyber and intelligence units, the Israel National Cyber Directorate (INCD), and various other intelligence agencies play a critical role.

A defining feature of Israel's cyber strategy is its extensive use of artificial intelligence to enhance both offensive and defensive cyber operations. AI technologies are employed to process vast quantities of intelligence data, in order to process identification of patterns, anomalies, and potential threats at a speed and scale beyond human capability. AI-driven tools are also integrated in offensive cyber operations such as development of adaptive malware, automated vulnerability discovery, and precision targeting of adversarial networks.

North Korea: The Democratic People's Republic of Korea (DPRK) maintains a distinct and highly centralized approach to cyber warfare, as a result of its strategic isolation and limited conventional economic resources. North Korea views Cyberspace as a cost-effective domain to gain more influence, gather intelligence, and surpass international constraints. One of the key institutions of North Korea in the matter of Cybersecurity is the Reconnaissance General Bureau (RGB) alongside other specialized cyber units that are often associated with groups such as the Lazarus Group. These bodies operate under strict state control and prioritize offensive capabilities such as financial cyber operations, and disruptive attacks targeting foreign institutions.

One of the central areas of AI application in North Korea is automated reconnaissance and vulnerability discovery. North Korean cyber units frequently use machine learning techniques to scan vast numbers of networks and systems for weaknesses which reduce the need for large human analyst teams and increases the speed of the identification of exploitable points. Additionally, that AI supports cryptocurrency related cyber operations and assists in tracking blockchain transactions, identifying vulnerabilities in crypto exchanges, and optimizing laundering techniques to obscure financial flows in the country's favor.

6.2.2 *Transparency in Reporting Cyber Incidents*

Transparency plays a key role in building trust among states and reducing the risk of escalation. When countries openly report cyber incidents and share relevant information, it becomes easier to identify threats, respond effectively, and avoid misinterpretation. In the DISEC context, promoting transparency also supports international cooperation and collective security. Mechanisms such as voluntary reporting frameworks and information-sharing platforms can strengthen global efforts to manage and mitigate cyber risks.

6.3 *Role of Non-State Actors in Cyber Warfare*

Non-state actors, such as hacker groups, activist organizations, and even terrorist networks, play an increasingly significant role in cyber warfare. Unlike states, they can operate flexibly and anonymously, targeting critical infrastructure, financial systems, or sensitive data to achieve political, economic, or ideological goals. Their actions often bypass traditional state controls, creating new challenges for international security and stability. As a result, addressing cyber threats now requires cooperation

not only between governments but also with private sectors and civil society to strengthen defenses and respond effectively. Understanding and monitoring these actors is essential to prevent large-scale disruptions and maintain global cybersecurity.

6.3.1 *Addressing the Threats Posed by Non-State Cyber Actors*

Non-state cyber actors, such as hacker groups, terrorist organizations, and independent individuals, pose a significant challenge to international security. Unlike states, these actors are often harder to identify, regulate, or hold accountable, which increases the risk of unpredictable cyberattacks. Within the framework of the United Nations General Assembly First Committee (DISEC), addressing these threats requires stronger international cooperation, improved intelligence sharing, and the development of legal mechanisms to track and respond to malicious activities. States are encouraged to work together to prevent these actors from exploiting gaps in cybersecurity systems.

Additionally, it is important for governments to strengthen their national cybersecurity infrastructure and enforce strict regulations to limit the activities of such groups. Public-private partnerships also play a key role, as many cyber systems are operated by private companies. By increasing awareness, investing in cybersecurity, and promoting global norms of responsible behavior, the international community can reduce the risks posed by non-state cyber actors and enhance overall digital security.

6.3.2 *Private Sector Accountability*

Private secretaries play an important role in supporting high-level officials and managing sensitive information. Their responsibilities require professionalism, confidentiality, and ethical behavior. A lack of accountability can lead to misuse of information or abuse of authority.

Ensuring accountability means setting clear rules and oversight mechanisms. Regular monitoring and transparency help prevent misconduct and build trust. This is essential for maintaining integrity within institutions.

6.4 *Cybersecurity Gaps Between Developed & Developing Nations*

Cybersecurity gaps between developed and developing nations remain a critical issue in the context of cyber warfare, particularly under the DISEC agenda. Developed

countries typically have stronger digital infrastructure, advanced defense systems, and greater investment in cybersecurity, enabling them to better prevent and respond to cyber threats. In contrast, developing nations often struggle with limited funding, outdated technology, and a lack of trained cybersecurity professionals.

These weaknesses make them more vulnerable to cyberattacks, such as hacking, data theft, and disruptions to essential services like energy and communication systems.

Furthermore, insufficient legal frameworks and limited participation in international cybersecurity initiatives hinder their ability to effectively combat cyber threats. This imbalance increases global insecurity, as cyber warfare can exploit the most vulnerable states, emphasizing the importance of international cooperation, capacity-building, and knowledge-sharing to bridge this divide.

6.4.1 *Funding Limitations in Cyber Defense*

Funding limitations in cyber defense pose a significant challenge for many states, particularly within the context of cyber warfare discussed in DISEC. Effective cybersecurity requires continuous investment in advanced technologies, skilled personnel, and infrastructure upgrades. However, many countries—especially developing ones—struggle to allocate sufficient financial resources due to competing national priorities such as healthcare, education, and economic development.

As a result, their cyber defense systems may remain outdated, leaving critical infrastructure and government networks vulnerable to attacks. Limited funding also affects the ability to train cybersecurity experts, conduct research, and participate in international cooperation efforts. This financial gap not only weakens national security but also creates opportunities for malicious actors to exploit less-protected systems, highlighting the need for increased international support, public-private partnerships, and more equitable distribution of cybersecurity resources.

6.4.2 *Establishing International Cyber Training Programs*

Establishing international cyber training programs is a key step in strengthening global resilience against cyber warfare within the DISEC agenda. Many countries, particularly developing nations, lack access to skilled cybersecurity professionals and

up-to-date technical knowledge needed to effectively prevent and respond to cyber threats. International training programs can help bridge this gap by providing standardized education, hands-on experience, and knowledge-sharing between states.

Such initiatives can be facilitated through partnerships between governments, international organizations, and the private sector, ensuring that participants gain exposure to the latest technologies and best practices. Additionally, these programs promote trust and cooperation among nations, which is essential in addressing cross-border cyber threats. By investing in capacity-building through training, the international community can reduce vulnerabilities, enhance collective security, and create a more coordinated global response to cyber warfare.

***6.5** Effects of Advancing Technology and New Technological Developments on Cyber Warfare*

Advancing technology has made cyber warfare faster and harder to detect. Tools like artificial intelligence and automation allow actors to carry out large-scale cyberattacks and data breaches. This enables conflicts to happen across borders with low cost and risk.

At the same time, these developments have improved cybersecurity systems. Governments and organizations can now detect and respond to threats more quickly. However, this creates an arms race between attackers and defenders, making regulation and cooperation more difficult.

***6.5.1** Regulating Artificial Intelligence in Cyber Warfare*

Artificial intelligence (AI) is rapidly transforming the nature of cyber warfare by enhancing the speed, scale, and sophistication of offensive and defensive operations. AI-driven systems are capable of automating vulnerability detection systems, conducting large scale cyber intrusions and generate highly convincing disinformation. At the same time, AI is increasingly used for defensive purposes by numerous countries, especially in fields of threat detection and real-time response to cyber incidents.

The integration of AI into cyber operations raises significant legal, ethical, and strategic concerns.

Difficulty of attribution, the risk of unintended escalation due to autonomous decision making systems, and the use of AI technologies in harmful intent are some of many other disability risks. Additionally, the nature of many AI models, particularly in machine learning, complicates accountability and compliance with existing frameworks of international law, including principles related to sovereignty, proportionality, and distinction.

Nonetheless, there is growing recognition within the international community of the need to develop common standards and transparency initiatives to reduce risks, prevent misuse, and promote stability in cyberspace. It is critical that universally accepted norms or binding agreements to be formed and deployed for the rightful assessment of the increasing influence of AI in Cyberspace.

6.5.2 *The effect of digital media elements on misinformation and intelligence leaks*

Digital media elements such as social media platforms and online news sources play a major role in spreading misinformation and internet leaks. Information can be shared rapidly and reach large audiences without proper verification. This increases the risk of false narratives, manipulation, and the quick spread of sensitive data.

At the same time, these platforms can help raise awareness and provide real-time information. However, the lack of strict control and fact-checking makes it difficult to prevent misuse. This highlights the need for stronger regulations and responsible digital media use.

7) Relevant International Organizations and NGOs

7.1 *The United Nations Office for Disarmament Affairs (UNODA)*

The United Nations Office for Disarmament Affairs (UNODA) is responsible for supporting disarmament initiatives and strengthening international security within the United Nations framework. UNODA works closely with governments, international organizations, and experts to provides policy guidance, research support, and technical expertise to assist Member States in developing arms control measures and cooperative approaches aimed at reducing global security risks.

In response to emerging challenges such as cyber warfare, the office also supports international discussions on responsible state behavior in cyberspace and promotes cooperative measures designed to prevent conflict escalation.

Duties of UNODA

- Assisting Member States in implementing disarmament treaties and agreements
- Promoting global disarmament efforts
- Providing policy advice and technical expertise to United Nations bodies
- Maintaining disarmament information systems and reporting mechanisms

7.2 *European Union Agency for Cybersecurity (ENISA)*

The European Union Agency for Cybersecurity (ENISA) is responsible for supporting cybersecurity development and cooperation within the European Union. The agency provides expertise, policy recommendations, and technical assistance to strengthen digital resilience and improve responses to cyber incidents. ENISA works closely with governments and private sector actors to enhance preparedness, protect critical infrastructure, and promote coordinated approaches to cybersecurity challenges.

DUTIES OF ENISA

- Organizing cyber crisis simulations and exercises
- Developing cybersecurity certification frameworks
- Publishing threat intelligence reports and guidelines
- Assisting in the implementation of EU cybersecurity laws and regulations

7.3 *North Atlantic Treaty Organization (NATO)*

The North Atlantic Treaty Organization (NATO) is a political and military alliance established in 1949 to promote collective defense, stability, and security cooperation among its member states. Within its institutional framework, NATO coordinates joint security policies, strategic planning, and defense cooperation aimed at maintaining international peace and safeguarding member nations against emerging threats.

In addition to its traditional military responsibilities, NATO has increasingly prioritized cybersecurity and recognized cyberspace as an operational domain as cyber threats have become a significant challenge to global security.

DUTIES OF NATO

- Intelligence sharing and threat information exchange among member states
- Protection of critical military and civilian infrastructure
- Operating specialized cyber defense institutions (e.g: CCDCOE)
- Developing common cybersecurity standards, policies, and operational guidelines

7.4 *The International Telecommunication Union (ITU)*

The International Telecommunication Union (ITU) is a specialized agency of the United Nations responsible for coordinating global telecommunications and information and communication technologies (ICTs). Established in 1865, the organization works to develop international technical standards, expand global connectivity, and promote cooperation among states in the management of digital communication networks.

In the context of cybersecurity and cyber warfare, the ITU plays a critical role by developing international norms, guidelines, and best practices to protect digital networks and ensure secure communication channels.

DUTIES OF ITU

- Develops international technical standards for telecommunications and ICTs
- Providing platforms for dialogue and coordination among governments, private sector actors, and international organizations
- Coordinating international spectrum management and satellite communications
- Publishing research, guidelines, and threat-related resources (e.g: GCI)

7.5 *Global Forum on Cyber Expertise (GFCE)*

The Global Forum on Cyber Expertise (GFCE) is an international platform established in 2015 to strengthen global cooperation in cybersecurity capacity building. GFCE brings governments, international organizations, private sector actors, and technical experts together to support the development of national and regional cybersecurity strategies, share knowledge, and implement practical solutions.

DUTIES OF GFCE

- Coordinating global initiatives to strengthen cybersecurity expertise and assisting governments
- Providing guidance, resources, and collaborative programs
- Organizing international conferences, workshops, and training programs
- Endorsing cybersecurity needs with available resources

7.6 *The CyberPeace Institute*

The CyberPeace Institute is an international non-profit organization established in 2019 to promote a safer and more secure cyberspace. The institute brings together governments, private sector actors, civil society, and technical experts to support the protection of vulnerable communities from cyberattacks and to enhance accountability for malicious cyber activities. It operates by conducting research and analysis, providing operational support to victims of cyber incidents, and facilitating collaboration among stakeholders to strengthen cyber resilience.

DUTIES OF CYBER PEACE INSTITUDE

- Providing independent research and evidence based reports regarding cyber security
- Analyzing and documenting the affects of cyberattacks on society
- Advocating the protection of civilians/civilian infrastructure in cyberspace and supporting victims of cyberattacks
- Raising global awareness about cyber harm and risks

8) Topics a Resolution Should Address

1.To what extent are States cooperating to prevent cyberattacks that threaten international peace and security, including attacks on critical infrastructure such as energy systems, healthcare networks, and financial institutions?

2. How can international legal frameworks and existing norms be strengthened to regulate state behavior in cyberspace and prevent the escalation of cyber conflicts between States?

3. How can international cooperation be promoted to identify and investigate cross-border cyber crimes and cyber terrorism?

4. What measures should States take to protect critical infrastructure such as government systems, communication networks and transportation systems against cyber threats?

5. What capacity-building initiatives can be implemented to help developing countries strengthen their national cybersecurity strategies, technical infrastructure and their capacity to respond to cyberattacks?

6. How can the international community address cyber warfare threats such as cyber operations being used as political pressure, espionage or military strategy tool?

7. What mechanisms can be improved to promote responsible state behavior in cyberspace and ensure accountability for malicious cyber activities?

8. In what ways can cooperation between states, international organizations and the private sector to strengthen global cyber security and increase information sharing?

9. What steps can be taken to combat the spread of disinformation, cyber propaganda and other malicious online activities that may threaten political stability and democratic institutions?

10. How can international confidence building measures and transparency mechanisms be improved to reduce distrust between states and prevent cyber incidents from escalating into larger conflicts?

9) Conclusion

In conclusion, the issue of Cyber warfare remains a critical challenge for the international community, requiring urgent and coordinated action. Despite existing efforts and regulations, significant gaps and risks still persist. Therefore, it is essential for member states to collaborate, strengthen international frameworks, and develop effective and sustainable solutions. Delegates are expected to carefully analyze the root causes of the issue and propose innovative and practical resolutions during the committee sessions.

10) Bibliography

https://www.un.org/

https://www.un.org/en/ga/first/

https://en.wikipedia.org/wiki/Cyberwarfare

https://www.fortinet.com/resources/cyberglossary/cyber-warfare

https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberwarfare.html

https://www.cisecurity.org/cybersecurity-threats

https://cyberpeaceinstitute.org/

https://thegfce.org/

https://www.itu.int/home/

https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence

https://www.enisa.europa.eu/

https://disarmament.unoda.org/en/updates/cyber-threats-information-weapon