GA1 – DISEC
STUDY GUIDE

(Disarmament and International Security Committee)

KARABUK UNIVERSITY

MUN

MODEL UNITED NATIONS

Bu Program Gençlik ve Spor Bakanlığı Tarafından Desteklenmektedir

www.moderndiller.net

Letter from Modern Languages

Most Esteemed Delegates,

It is my great honor to welcome you all to KBUMUN'26 as the Club Manager of this distinguished event. On behalf of our Executive Board and organizing team, I am delighted to invite you to an intellectually stimulating and globally engaging experience.

KBUMUN is more than an event; it is a platform where ideas are exchanged, perspectives are broadened, and leadership skills are cultivated. Throughout the sessions, you will have the opportunity to enhance your diplomatic abilities, engage in constructive debate, and collaborate with peers from diverse backgrounds. We strongly believe that the discussions and experiences you gain here will contribute significantly to your personal and academic growth.

We are confident that KBUMUN'26 will be a memorable journey filled with learning, collaboration, and inspiration. I eagerly look forward to witnessing your contributions and to meeting each one of you before I complete my Modern Languages Journey continuing for 4 years. It will be an amazing goodbye to this club.

Yours sincerely,
Hakan Acar,
Secretary-General/Club Manager,
hakan@moderndiller.net
KBUMUN'26

Introduction to DISEC Comittee

The United Nations (UN) Disarmament and International Security Committee (DISEC) was established as the first of the six main committees in 1945 at the signing of the charter of the United Nations. DISEC was created because there was a need for an international platform to have conversations around peace and security of our global community members. The purpose of DISEC in the UN General Assembly, according to the UN Charter, is to establish general principles for cooperation in maintaining international peace and security. This includes principles for disarmament and controlling armaments. The committee also makes recommendations about these principles to the Security Council members. Furthermore, it addresses important international security issues and demilitarization in all countries and regions. It is committed to ensuring that people around the world remain safe.

Agenda Item: *Addressing the Security Implications of Emerging Technologies and Strengthening Cyber Resilience in Conflict Zones*

Introduction to Topic

With new technologies and the growing personalization of computers in this century, people now have access to more knowledge than ever before. This access creates many opportunities for countries and international organizations to invest in different areas. While the digital world brings many benefits, it also raises concerns about personal data being sold or stored for the benefit of large technology companies. Algorithms can sometimes predict personal preferences better than individuals themselves. There are also growing risks, such as cyber warfare, the misuse of AI in military operations, and threats to international stability.

Before the Second World War, cryptography was mainly used to protect government communications and war strategies. Today, most personal data is stored in the cloud, and if this data is not properly protected, it can pose serious risks to individuals and even entire countries.

A conventional computer utilizes bits for data storage. Bits are represented as 1 or 0, which constitutes a binary system. In quantum computing, the system utilizes electrons, referred to as qubits in this context. An electron is a particle inside the Standard Model, and classical physics principles do not govern particles. In Quantum Mechanics, statistical charts are utilized to predict position or momentum. A cubit, representing an electron, possesses a statistical chart and can assume any value between 0 and 1. A quantum computer, due to its rapid statistical computation capabilities, may efficiently decipher contemporary encrypted data.

Updated Definitions for Clarity

- **Cybercrime**: This term covers a wide range of unlawful actions that are done using digital equipment and/or networks. These crimes employ technology to commit fraud, steal identities, hack into computers, spread viruses, and other bad things. Cybercriminals use flaws in computer networks and systems to get into them without permission, steal private information, disrupt services, and hurt people, corporations, and governments financially or in terms of their reputation.

- **Cyber Resilience**: The ability to keep electronic data and systems safe from cyber attacks and get back to business swiftly after a cyber attack.

- **Security Implications:** The possible dangers and effects that come from the system's weaknesses.

- **Artificial Intelligence (AI)** is the technology that lets computers and machines act like people when it comes to learning, understanding, solving problems, making decisions, being creative, and being independent.

- **Internet of Things (IoT):** The whole network of connected devices and the technology that lets them talk to each other and to the cloud.

- **Cryptography** is the art of making and comprehending codes that keep information private.

- **Sparta** is an old Greek city in the southern Peloponnese. It is known for the strictness and military skill of its people and their simple way of life.

- **Standard Model:** The Standard Model of particle physics is the theory that classifies all known elementary particles and describes three of the four fundamental forces in the universe. These forces include electromagnetic, weak, and strong interactions, with gravity being the only one that is not included in the Standard Model. Over the course of the second half of the 20th century, it was gradually developed with the assistance

of a large number of scientists from all over the world. In the middle of the 1970s, once the existence of quarks was demonstrated by experimental evidence, the present formulation was completed completely. Since then, the Standard Model has been given more support as a result of the discoveries of the top quark (1995), the tau neutrino (2000), and the Higgs boson (2012). In addition, the Standard Model has been able to precisely predict the W and Z bosons, in addition to a variety of features associated with weak neutral currents.

- **Bit**: What is a binary digit, or bit? A computer can process and store data at the smallest unit known as a bit, or binary digit. There are always two possible physical states for a bit, much like an on/off switch. The state is represented by a single binary number, usually a 0 or 1.

- **Qubit:** In quantum computing, a qubit, sometimes called a quantum bit, is the basic building block of quantum information. The conventional binary bit is physically represented using a two-state gadget, and this is its quantum analogue. A qubit, a two-state (or two-level) quantum mechanical system, is one of the simplest examples of a system displaying the quirks of quantum physics. Examples include the polarization of a single photon, in which the two spin states may also be measured as horizontal and vertical linear polarization, and the spin of an electron, in which the two levels can be read as spin up and spin down. Both of these examples are examples of phenomena that can be observed. In order for a bit to be in a classical system, it would have to be in one of two states. Nevertheless, the capacity of the qubit to exist in a coherent superposition of numerous states at the same time is a key trait of both quantum computing and quantum physics. This ability is a fundamental characteristic of both fields.

History of the Topic

The present knowledge of cryptography is dependent on the mechanics of the 20th century, electromagnetic technologies such as the Enigma rotor machine, and the 20th century. On the other hand, the history of cryptography goes back considerably further than that. The first known examples of cryptography may be traced back to the Old Kingdom of Egypt, which was located in ancient Egypt.

- **Cryptography Old Kingdom of Egypt**

  Cryptography Old Kingdom of Egypt Hieroglyphs were a sophisticated system used for written communication in ancient Egypt that did not rely on a conventional alphabet. To ensure that their knowledge was shielded from other civilizations, only a limited number of people were allowed to study and practice this type of writing. Without specialized knowledge, deciphering hieroglyphic writing was extremely challenging due to its intricacy. Modern technology has advanced, but it wasn't until the Rosetta Stone was unearthed that the secret to deciphering hieroglyphics was found. Three different scripts were used to engrave this artifact: Greek, Demotic (a script used by the Greeks and in later periods of ancient Egypt), and hieroglyphic. Scholars used Greek text as a reference because the Ancient Greek and Modern Greek alphabets were similar, which greatly aided in the interpretation of hieroglyphic inscriptions.

- **Scytale**

  The scytale, a cryptographic device, was employed for secure military communication in ancient Greece, particularly in Sparta.

  This method involved wrapping a cylindrical wooden rod with a strip of parchment or leather. The characters appeared disordered and incomprehensible when the message was inscribed along the length of the rod and subsequently unwound. Confidentiality in military correspondence was maintained by necessitating that the designated receiver decrypt the message via a scytale of identical size.

- **A Cipher of Caesar**

  This is the method that was initially implemented in Ancient Rome, under the reign of Caesar. During the process of military communication, Caesar and his generals altered the letter sequence in order to generate encrypted text. This was done in order to ensure that the message that they were conveying was not understood by the opposing troops. The alphabet was written down twice, and then a certain amount of letters were moved to the right in order to obtain this script.

- **A Book of Messages in Cryptographic Form**

  The author of this work, which is considered to be the birthplace of contemporary encryption, is Al-Khalil. This book is the first of its kind to contain cryptographic method codes in a detailed and organized manner.

- **Subh al-a'sha**

  The author of this encyclopedia, Ahmad al-Qalqashandi, has compiled it into fourteen volumes. Ibn al-Durayhim is the source of the information that is required for this, however his cryptography works have been misplaced. For that, you need to have all of the knowledge up until that point.

- **Homophonic Substitution Cipher**

  It is possible to increase the level of security and complexity of the messages that are encoded by employing the homophonic substitution cipher. This is accomplished by using numerous symbols to represent individual letters. At the beginning of the 1400s, the Duke of Mantua was the first person to use this innovative strategic approach. Its advanced character, which places it ahead of its time in the development of cryptography, is a result of the fact that it combines both monoalphabetic and polyalphabetic encryption algorithms.

- **Cryptography 1800 to World War I**

  The initial cryptanalysis originated in the 19th century. Cryptanalysis is the discipline of identifying vulnerabilities within cryptographic systems. Examples of these efforts include Charles Babbage's mathematical cryptanalysis of polyalphabetic ciphers during the Crimean War and the comprehension of cryptanalysis. Auguste Kerckhoffs' cryptographic publications in the late 19th century. Edgar Allan Poe, a renowned author of crime novels, employed methodical techniques to decipher codes in the 1840s.

- **The Enigma Rotor Machine**

  Nazi Germany employed the Enigma rotor machine during World War II to secure military and diplomatic communications. This powerful encryption technology utilized a 26-letter alphabet to turn each input letter into a corresponding number value. By inputting the accurate decryption code, the machine's encoding system could revert the transformation, ensuring secure communication during the conflict.

- **Allies**

  The Americans designated the intelligence derived by cryptanalysis, while the prior British word for Ultra was 'Boniface,' intended to imply that, if compromised, it might be attributed to a singular agent as the source. This is an electromagnetic apparatus featuring a rotor configuration akin to the Enigma, however significantly enhanced. Neither is reported to have been breached by anyone during the War. The computerized world established post-World War II encompasses numerous intricate cryptographic methods. This system typically employs two chips. These chips are referred to as the Public Key and the Private Key.

- **Public Key Cryptography**

  Asymmetric cryptography is another name for this system. Each key pair consists of a matching private key and a public key. Key pairs are produced using cryptographic techniques based on mathematical problems called one-way functions. Public-key cryptography can share the public key without compromising security, but the private key must be kept confidential.

- **Symmetric Key Cryptography**

  Methods that use the same cryptographic keys for both plaintext encryption and cipher text decoding. The two keys may be identical or just transformed from one to the other. The keys actually represent a shared secret that may be used by two or more persons to maintain a confidential information relationship. The requirement that both parties have access to the secret key is one of the main drawbacks of symmetric-key encryption compared to public-key encryption, also known as asymmetric-key encryption. However, symmetric-key encryption techniques are usually better for bulk encryption. With the exception of the one-time pad, its smaller keys allow for quicker transmission and less storage. Artificial Intelligence (AI) and Quantum Computers are examples of emerging technologies that are making this system more vulnerable and ineffective. New technologies began to appear in order to preserve security.

Current Situation

LulzRaft

In 2011, a hacking group or individual going by the name LulzRaft attracted headlines from around the world when they targeted Canadian institutions like the Conservative Party of Canada and Husky Energy. On June 7, they falsely claimed that Prime Minister Stephen Harper had been admitted to the hospital after choking on a hash brown on the Conservative Party website. Before it was discovered, the fake momentarily tricked even federal authorities.

The next day, LulzRaft gained access to private data, including names and contact information, by breaking into a database of Conservative Party donors. The organization said that simple methods were sufficient for the intrusion and blasted the party's insufficient security procedures. In addition, as a sarcastic gesture connected to their earlier attack, they broke into Husky Energy's website and displayed a fake advertisement for free gas.

Operation Ababil

Operation Ababil The "Cyber Fighters of Izz Ad-Din Al Qassam," also known as the Qassam Cyber Fighters, carried out a number of cyberattacks in 2012. Major US financial institutions including J.P. Morgan Chase and the New York Stock Exchange were the targets of these denial-of-service assaults.

On September 18, 2012, the group declared their intentions, justifying them with criticism of the contentious Innocence of Muslims video. The attacks ended on October 23, 2012, which coincided with the Eid al-Adha festival, despite only slightly disrupting the targeted websites. Following this, the organization said that it would be open to email correspondence with the media.

Shamoon

W32, or Shamoon Shamoon. A damaging computer virus called DistTrack targets Windows versions that use the 32-bit NT kernel. The discovery occurred in 2012. Infected systems become inoperable as it propagates over networks, uploads and removes files, and modifies the master boot record. The virus was used in major cyber attacks against Saudi Aramco and RasGas in Qatar, and the group "Cutting Sword of Justice" claimed responsibility for breaching 30,000 Aramco workstations. It was dubbed one of the largest cyber attacks

ever and linked to malware such as Flame. Shamoon returned in 2016 and then again in 2017 and 2018.

Stuxnet

It is believed that Israel and the United States have been working together since 2005 to create the malicious worm known as Stuxnet, which was discovered in 2010 as part of Operation Olympic Games. It targets SCADA systems, specifically Siemens programmable logic controllers (PLCs), with the intention of interfering with industrial processes. Most importantly, it allegedly damaged Iran's nuclear program by causing centrifuges to malfunction.The worm exploits zero-day vulnerabilities in Microsoft Windows systems and propagates throughinfected USB drives. It compromises PLCs and degrades physical equipment by altering code while hiding its functions. Stuxnet infected over 200,000 computers and destroyed nearly 1,000 machines, demonstrating its ability to target critical infrastructure outside of nuclear facilities.

Past Actions

China: The People's Republic of China attained nuclear weapon status by executing its inaugural nuclear test in 1964. In the 1980s, following Mao's death, proposals concerning the utilization of nuclear weapons began to emerge. China's nuclear posture and policy were officially articulated in white papers initiated in 1995, which disclosed the nation's perceptions and strategies on national security. The notion of "limited deterrence" served as a benchmark in the ideas for China's nuclear military policySince the early 2000s, China has prioritized cyber security as a crucial component of its national strategy. State-sponsored hacking groups were employed to conduct espionage and enhance their cyber threat capabilities by targeting Google and other American corporations during the 2010s. Throughout the years, it has employed cyber-attacks to incapacitate power plants, communication networks, and transportation systems during conflicts. The guidelines established for the creation of cybersecurity regulations within the UN have exhibited reluctance to ensure the preservation of state control.

Iran: Iran commenced nuclear development in 1957 under the US Atoms for Peace initiative. It acceded to the Nuclear Non-Proliferation Treaty in 1970 and thereafter boosted its investment in the advancement of nuclear technology for peaceful use. Subsequently, it partnered with Western nations and the United States, formalizing agreements with Germany for nuclear reactors intended for energy research. However, it was in the 2000s that Iran emerged as a key player in the 2015 Joint Comprehensive Plan of Action (JCPOA), amidst suspicions regarding the development of nuclear weapons by the P5+1 countries. This accord restricted Iran's nuclear development; nonetheless, tensions escalated with the US withdrawal in 2018.

In the realm of cyber warfare, Iran has emerged as a significant actor, executing several operations, particularly against the infrastructures of the United States and Israel, indicating that Iran perceives cyberspace as an integral component of its military apparatus. Cybersecurity is essential, and Iran has deemed it a national defense initiative; hence, significant emphasis is placed on enhancing its capabilities. Concurrently, based on the principle of cyber sovereignty, it rejects any external involvement in the cyber realm. The utilization of cyber technology for both Iran's security and to gain an advantage over its adversaries contravenes the peaceful norms upheld by the UN.

Italy: Italy initiated its initial engagement with nuclear power in the 1950s. Throughout the Cold War, it collaborated closely with the United States as a member of NATO. Nuclear energy production was established, and nuclear power stations were constructed between 1950 and 1960. Nevertheless, it was not classified as a nuclear-armed state and acceded to the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) in 1975. The nation sustained energy production for years without advancements in military capabilities; nevertheless, in 1987, subsequent to the Chernobyl tragedy, it resolved to shut down all nuclear power facilities following a referendum. Subsequent to this period, it primarily satisfied its energy requirements through imports and renewable energy sources.

In the early 2000s, Italy resolved to address the global proliferation of cyberspace. In 2017, it endeavored to safeguard state institutions and vital infrastructures by establishing the National Cyber Security Framework. The nation has endeavored to enhance its cybersecurity for several years, having been a target of cyberattacks in Europe in recent years. Italy,

exemplifying a nation affected by emerging technologies and cyber attacks, routinely addresses these concerns within NATO and the UN, advocating for the ethical and regulated use of such technology to mitigate their detrimental impacts on people. A notable demonstration of its commitment to public welfare is its proposal for a "Cyber Ceasefire Agreement" to the UN, following the impact of the 2021 cyber attack on hospital systems.

Conclusion

Disarmament and international security are fundamentally interconnected pillars of global peace and security.

Effective disarmament reduces the chance of armed conflict, curtails the proliferation of weapons of mass destruction, and diminishes the risk of catastrophic consequences from militarization. Simultaneously, enhancing international security through trust-building, diplomacy, and adherence to international regulations fosters an environment favorable to disarmament. Nations must pledge to transparency, reciprocal respect, and collaboration to attain sustainable development, while recognizing that global security is a collective obligation. By prioritizing disarmament, the international community can foster a safer and more peaceful world, securing tranquility for future generations.

Guiding Questions

1. *How can governments find a balance between people's right to bear guns and public safety?*
2. *How can users be educated to improve their knowledge and resilience to cyber risks on social media?*
3. *What novel technologies or tactics can be used to detect and mitigate cybersecurity threats in social media?*
4. *What are the most common cybersecurity vulnerabilities confronting social networks today?*
5. *What flaws exist in the cryptographic systems of today, and why are they deemed insufficient in light of new developments?*
6. *How have these countries used strategic initiatives or attacks to showcase their cyber capabilities?*
7. *Can countries follow a common protection path against cyber attacks that have occurred in the past and present years, and how?*