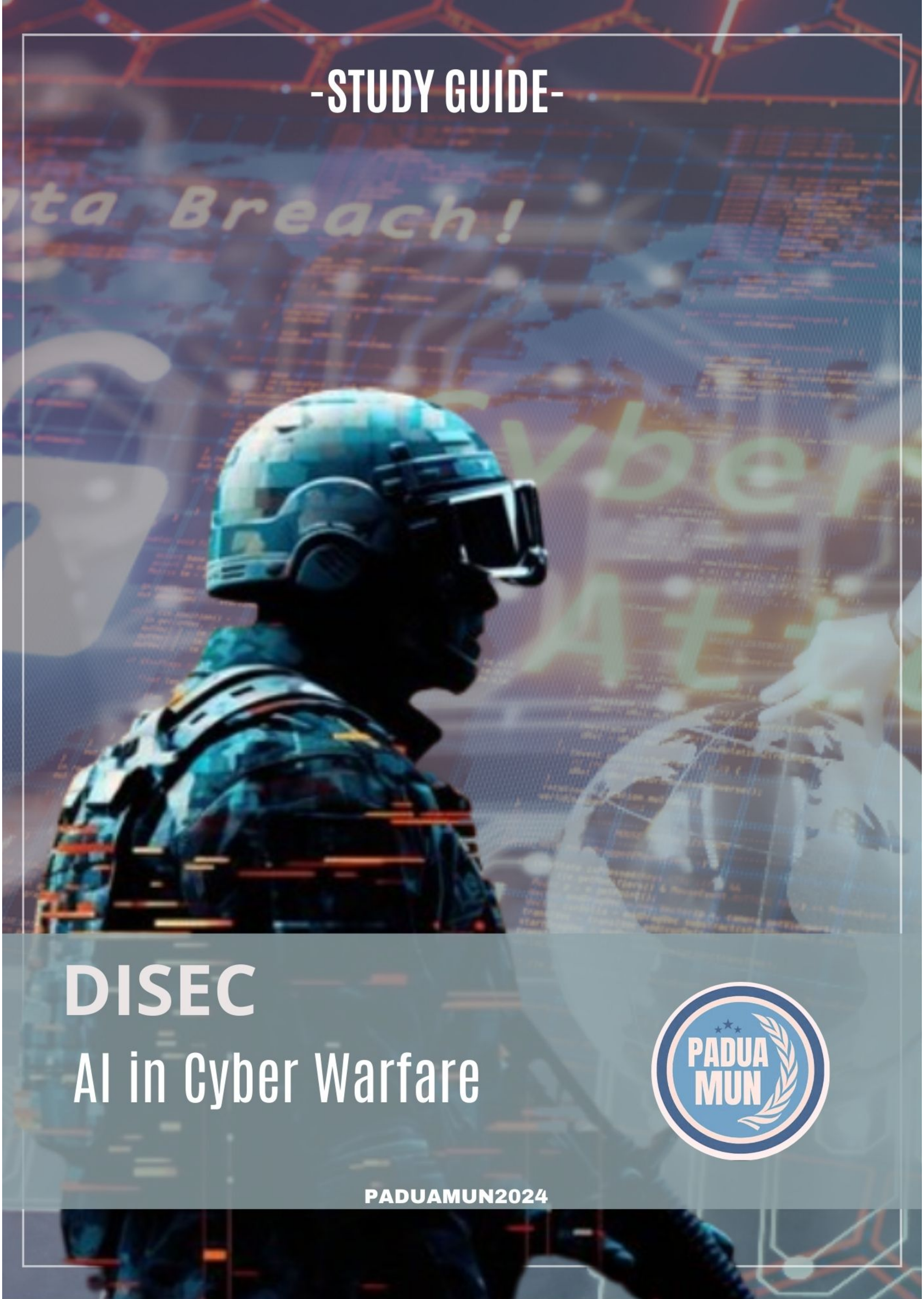
-STUDY GUIDE-



# DISEC

## AI in Cyber Warfare

PADUA MUN

PADUAMUN2024

# TABLE OF CONTENT

## Letter from the Secretary General

Hello and welcome to PADUAMUN 2024!  My name is Mariagrazia Elena Pascarella Burger, and I am thrilled and deeply honored to be your Secretary-General for the 2024 edition of PADUAMUN. The journey leading up to this moment has been filled with excitement and anticipation as our team has worked tirelessly to ensure that this year's conference surpasses all expectations. We have left no stone unturned in our quest to make PADUAMUN 2024 truly exceptional.

My Model UN journey started in 2021, my first Virtual MUN  where I received a Verbal Mention in the SOCHUM committee. But my first time enjoying and understanding what really Model United Nations is about was in the PADUAMUN 2022, I remember being extremely nervous from hours of practicing and memorizing, even tho I won Outstanding Delegate it was not until the  PUCPMUN in Lima that I understood that I didn't need to memorize everything or be so nervous, it was also there when found my committee Disec securing a Verbal Mention.  In 2023, my MUN journey expanded with participation in four conferences all of them being the Disec committees always working in doubles. In Lima, I attended NewtonMUN, SanSilvestreMUN, and MarkhamMUN, earning Honorable Mention, Best Position Paper Award, and Outstanding Delegate respectively. At PaduaMUN, I clinched the Best Delegate title. My most recent challenge was preparing and debating in the NHSMUN in New York, where I represented my skills in the LEGAL committee. As I look ahead to PADUAMUN 2024, To all participants, both seasoned veterans and newcomers alike, I offer a word of encouragement: seize this opportunity to shine. Showcasing your leadership, creativity, and collaboration skills will not only enrich your own experience but also contribute to the collective success of the conference. Together, let us engage in thought-provoking discussions, foster creative solutions, and forge lasting friendships. With that said, I extend my warmest wishes for a memorable and rewarding experience at PADUAMUN 2024. May this conference inspire you to reach new heights and leave an indelible mark on your MUN journey. I eagerly anticipate the vibrant debates, innovative ideas, and camaraderie that await us in August.

Until then, let us make PADUAMUN 2024 an unforgettable chapter in the annals of Model United Nations. I look forward to seeing you all in August!

## Letter from the Secretary General

Dear delegates, It is a pleasure to welcome you to the Disarmament & International Security Committee and introduce myself as the director of this committee. My name is Alessandra Cáceres and I'm delighted to be serving as your director in this edition of San Antonio de Padua Tarapoto 2024. Regarding myself, I am currently studying International Relations at Universidad Peruana de Ciencias Aplicadas, and I am interested in the implementation of public policies, cultural diplomacy, issues related to human rights such as social inclusion mechanisms, international security, global sustainability, gender equality, immigration policies, and vulnerable groups.

My MUN journey began in 2018, and over the past six years, my enthusiasm for debate has only grown. This passion led me to join the inter-university debate team, Peruvian Debate Society. With my team, I have had the privilege of traveling to various cities worldwide, from Paris to Boston or even Panama City, participating in all Harvard Conferences. Although I am not actively debating at the moment, I am a member of the Peruvian Debate Society's General Assembly, where I contribute to important decisions regarding the team's direction and activities. Transitioning to the topic, it is crucial for you to understand that artificial intelligence plays an increasingly significant role in modern international security. As we delve into our discussions, you will see how AI technology can influence disarmament efforts, surveillance capabilities, and cybersecurity measures. The integration of AI in military operations, for instance, presents both opportunities and challenges. While it can enhance operational efficiency and decision-making processes, it also raises ethical concerns and the potential for an arms race in AI-powered weaponry. Regarding how to achieve the best delegate prize, it is fundamental to follow diplomacy rules. For me, the best delegate is someone other than the one who speaks at any cost and without any sense, is the one who manages to provide an agenda and a valuable message for the committee. Believe me, once you start understanding the issue as a genuine concern for you, it will be easier to articulate your points effectively.

Please feel free to contact me at any time before the conference via email. I have been a scholar delegate too so I understand how frustrating it can get when you do not get some of the concepts of the study guide and the conference it's around the corner! Therefore, do not hesitate to reach out to me!

Best regards, Alessandra Cáceres Gallegos

## History of the committee

The United Nations (UN) Disarmament and International Security Committee (DISEC) was created as the first of the Main Committees in the General Assembly when the charter of the United Nations was signed in 1945.

DISEC was formed to respond to the need for an international forum to discuss peace and security issues among members of the international community. According to the UN Charter, the purpose of DISEC in the General Assembly is to establish 'general principles of cooperation in the maintenance of international peace and security, including the principles governing disarmament and the regulation of armaments and also to give "recommendations with regard to such principles to the Members or to the Security Council." However, the DISEC committee cannot intervene in the decision-making process of the Security Council, DISEC can suggest specific topics to consider.

DISEC is also an institution of the United Nations Office for Disarmament Affairs (UNODA), formally named in January 1998 after the Secretary-General's second special session on disarmament in 1982. All Member States and observers of the United Nations are automatically part of the DISEC committee. The committee also considers all disarmament and international security matters within the scope of the United Nations Charter or issues related to the functions of any other organ of the United Nations, as well as principles governing the regulation of armaments.

Nowadays, DISEC has gathered in 72 opportunities to discuss topics of high relevance to international peace and worldwide stability, eradication of weapons of mass destruction, illegal arms trade, cyber warfare and state capacity building and the peaceful uses of outer space, among others. The UNODA is concerned with disarmament at all levels—nuclear weapons, weapons of mass destruction, and conventional weapons—and assists DISEC through its work conducted in the General Assembly for substantive norm-setting support to further its disarmament initiatives.

## Introduction to the topic

The rapid evolution of technology in armament has always been a critical and concerning aspect of technological advancement globally. As the United Nations Secretary-General noted, arms control has consistently been driven by the need to stay ahead of the challenges to peace and security posed by scientific and technological progress. While revolutionary technologies offer significant benefits for humanity, their military applications can threaten international peace and security. The challenge lies in fostering understanding among stakeholders about these technologies and creating responsive solutions to mitigate associated risks.

This is particularly relevant today with the military applications of artificial intelligence. AI has become a central focus worldwide, permeating every facet of our lives, including the military. The UN adopts a cautious stance on this issue, advocating for the peaceful use of AI. However, given the inevitable incorporation of AI into defense and attack technology, it is equally imperative to establish clear regulations governing its use. The abrupt progress of AI offers extraordinary opportunities for development and innovation but also brings significant challenges and potential dangers. These issues are attracting considerable attention at the global governance level.

### History of the topic

Since the birth of this technology in the 1950's up until now, AI has had a lot to contribute to our universal development and innovation. The merging of AI and cyber warfare is not a recent phenomenon and cyber operations have been revolutionized by them.

The surge of artificial intelligence goes back to the 1950's, when a group of scientists, mathematicians and philosophers integrated the concept of this tool. Among them was a man whose idea was that if humans utilize reasoning and information for problem solving, machines should be able to do the same, this man was Alan Turing. This proposal constructed the basis for his 1950 paper called "Computing Machinery and Intelligence", in which he first introduced the concept of AI to the world.

In the 1980's artificial intelligence's usage was established in expert systems, which were designed to imitate human abilities regarding decision-making (notably in cybersecurity), to monitor network traffic, system activities and user manners. Despite the fact that these systems were groundbreaking for their time, if a threat wasn't in the database, the detection would fail. In this scenario, AI-driven security inaugurated itself gradually.

Between the late 1990s and early 2000s, AI began to evolve rapidly, and it started to play a role in Intrusion Detection Systems. Neural networks and machine learning were introduced and gaining popularity, not to mention new techniques were developed in order to analyze network traffic patterns and detect anomalies that might announce a security breach. Additionally, in the 2000s, the evolving landscape continued, as the use of machine learning techniques in cybersecurity increased, applying algorithms to analyze data patterns and identify potential threats. At the same time, systems such as Natural Language Processing were implemented. This contributed to the identification of suspicious patterns or malicious content, in addition, it worked as an additional layer of defense, being a game-changer for cyber attacks or phishing attempts. Other examples are the Convolutional Neural Networks, a class of neural networks, which helped in image and pattern recognition, being applied during phishing attacks .

In this framework, we understand the application of Ai fundamentally when it comes to integrating computer science and large datasets to enable problem-solving. It encompasses subfields, taking as an exemplification machine learning (ML), which are primarily linked to artificial intelligence. In essence, AI empowers machines, including weapons, to function with a type of human-type intelligence. Focusing on nowadays, present trends focus on using AI to automate cybersecurity tasks and combat cyber threats, where attackers exploit software vulnerabilities that users are unaware of, by detecting and responding to unusual activities that may signal a zero-day attack.

***AI'S role***

AI's role in cyberwarfare has expanded to utilizing it as a tool or it becoming a threat. As the threat landscape evolves, the framework demands advanced tools that can keep up with them and combat the threats. At the same time, AI enables parties to manage and mitigate the risks of cyber threats effectively.

AI's benefits have not just been taken into advantage by the cyber security sector, but from cyber attackers as well. These attackers have boosted their capabilities and evade governmental defenses more effectively, by allowing them to automate and scale their operations easily (including generating more advanced phishing or vishing attacks and automating tasks).

As attacks become more sophisticated, governments and their cybersecurity teams try to adopt artificial intelligence in their systems in order to enhance their defense strategies. AI has proven to be a fundamental ally in early threat detection and rapid incident response, as it is one of the most significant uses of AI in cybersecurity terms.  AI systems can analyze vast amounts of data in real time, identifying unusual patterns that might determine an ongoing attack. Moreover, machine learning (ML) algorithms enable defense systems to continuously improve their ability to recognize and block new threats more quickly and effectively,

### AI as a tool

When it comes to using AI as a tool in cybersecurity and defense matters we need to talk about its usage in a wide range of sectors.

Threat detection: Threat detection is one of the most common applications of AI in cybersecurity. AI can collect, integrate, and analyze data from hundreds of control points, including system logs, network flows, endpoint data, cloud API calls, and user behaviors. In addition to providing greater visibility into network communications, traffic, and endpoint devices, AI can also recognize patterns and anomalous movements to identify threats more accurately at scale. For instance, AI- and ML-powered systems can analyze software based on inherent characteristics, like if it’s designed to rapidly encrypt many files at once, and tag it as malware. In the case of a hacker trying to access a high level of confidential files with an employee account, it might indicate a possible threat. By identifying anomalous user behavior in real time, these AI-, or ML-, powered systems can block both known and unknown malware from executing, making it much more effective. AI algorithms can rapidly execute a response without the need of human intervention, by blocking suspicious activity or isolating affected devices.

Threat management: Another top application of AI in cybersecurity is threat management, which consists of analyzing cybersecurity situations, incident responders and threat hunters to prevent cyberattacks, detect cyberthreats and answer to security incidents. .

In this scenario, member parties’ security teams probably accumulate a wide pile of cases, including threat intelligence, to work through, and as the implementation of AI in these increases, the velocity of having to treat these cases increases altogether. In this circumstance, security teams’ best option is to respond with more AI.

AI and other advanced technologies could be used to supplement the efforts of the human experts in charge of the threat management process. AI can scan vast amounts of data to identify potential threats and filter out non-threatening activities to reduce false positives at a scale and speed that human defenders can’t match. By reducing the time required to analyze, investigate, and prioritize alerts, security teams can spend more time remediating these alerts.

Threat response: AI is also used effectively to automate certain actions to speed up incident response times. For example, AI can be used to automate response processes to certain alerts. Say a known sample of malware shows up on an end user’s device. Then an automated response may be to immediately shut down that device’s network connectivity to prevent the infection from spreading to the rest of the database.

AI-driven automation capabilities can not only isolate threats by device, user, or location, they can also initiate notification and escalation measures. This enables security experts to spend their time investigating and remediating the incident.

**AI as a threat**

Now, on the other side of the coin, AI can also be used in a negative way, within these usage, there are various examples.

Cyber attacks optimization: Experts say that attackers can use generative AI and large language models to scale attacks at an unseen level of speed and complexity. Moreover, AI's usage contributes to increasing the efficiency of certain sectors regarding cyber operations such as reconnaissance, phishing, coding and ransomware techniques by polishing them with generative AI.

Automated malware: Experts say that in the near future, it may help software developers, computer programmers, and coders or displace more of their work. AI helps cybercriminals create variants of malware automatically, which, additionally, helps create various attacks with different characteristics that distinguish each other. Moreover, it also might be used during evasion techniques while trying to modify a malware to avoid detection. These developments are just for now, AI-powered tools may allow developers with entry-level programming skills to create automated malware in the future.

AI privacy risks: Despite the fact of fixing a bug, AI still poses privacy risks due to the vast amount of data it processes. For instance, a hacker breaching an AI system could gain access to various sensitive information types. AI systems used for surveillance or profiling could threaten privacy in many aspects. In some countries, AI profiling technology is already enabling states to invade user privacy.

Stealing AI models: There are some risks of AI model theft through network attacks, social engineering techniques, and vulnerability exploitation by threat actors such as state-sponsored agents, insider threats like corporate spies, and run-of-the-mill computer hackers. Stolen models can be manipulated and modified to assist attackers with different malicious activities, compounding artificial intelligence risks to society.

Data manipulation and data poisoning: While AI is a powerful tool, it can be vulnerable to data manipulation. After all, AI is dependent on its training data. If the data is modified or poisoned, an AI-powered tool can produce unexpected or even malicious outcomes.

In theory, an attacker could poison a training dataset with malicious data to change the model's results. An attacker could also initiate a more subtle form of manipulation called bias injection. Such attacks can be especially harmful in industries such as healthcare, automotive, and transportation.

Impersonation: You don't have to look further than cinema to see how AI-powered tools are helping filmmakers trick audiences. For example, in the documentary Roadrunner, the late celebrity chef Anthony Bourdain's voice was controversially created with A.I.-generated audio and easily tricked viewers. Similarly, the veteran actor, Harrison Ford, was convincingly de-aged by several decades with the power of artificial intelligence in Indiana Jones and the Dial of Destiny.

People can also use free AI-powered tools to create remarkably realistic fake voices trained on mere seconds of audio.

Law enforcement believes that in addition to virtual kidnapping schemes, AI may help criminals with other types of impersonation fraud in the future, including grandfather scams. Generative AI can also  produce text in the voice of thought leaders. Cybercriminals can use this text to run different types of scams, such as fraudulent giveaways, investment opportunities, and donations on mediums like email or social media platforms like Twitter.

More sophisticated attacks: As mentioned, threat actors can use AI to create advanced malware, impersonate others for scams, and poison AI training data. They can use AI to automate phishing, malware, and credential-stuffing attacks. AI can also help attacks evade security systems like voice recognition software in attacks called adversarial attacks.

**Impact of AI:**

In the rapidly evolving landscape of cyber warfare, artificial intelligence (AI) has emerged as a transformative force. This cutting-edge technology has drastically changed the dynamics of cyber conflicts, offering both opportunities and challenges in the digital battleground. AI's impact on cyber warfare is profound, reshaping strategies, enhancing capabilities, and introducing new forms of digital confrontations. One of the most significant ways AI transforms cyberwarfare is by developing autonomous hacking systems. These AI-powered tools can identify vulnerabilities, exploit weaknesses, and adapt strategies based on the target's response. Also, AI algorithms can be utilized by attackers to identify patterns in security systems. This enables cybercriminals to launch sophisticated attacks.

Human capabilities alone are no longer sufficient to secure against attacks, making AI crucial for monitoring and detecting threats to enhance defense measures. Additionally, AI can aid in identifying and prioritizing risks by guiding incident responses, and spotting malware attacks before they happen.

## ***Past Actions***

AI is quite a recent matter in the United Nations discussion table. The resolution on "Enhancing International Cooperation on Capacity-building of Artificial Intelligence" emphasizes that the development of artificial intelligence should adhere to "the principles of being human-centered," promoting beneficial intelligence, and benefiting humanity.

It encourages international cooperation and practical actions to help countries, especially developing countries, strengthen their AI capacity building, enhance their representation and voice in global AI governance, advocate for "an open, fair, and non-discriminatory business environment," and support the United Nations in playing a central role in international cooperation.

The resolution aims to achieve inclusive, beneficial, and sustainable development of artificial intelligence, thereby contributing to the realization of the United Nations' 2030 Agenda for Sustainable Development.

## ***Current Situation***

Artificial intelligence is increasingly used within the scope of cyber warfare around the world. Far more now in this new cyber era and in the context in which the vast majority of countries have developed artificial intelligence as an attack and defense mechanism. In today's world, it's difficult to identify a domain, system, or problem that doesn't utilize, incorporate, or could benefit from AI. From its early development stages, AI techniques and technologies have been successfully employed by military forces for various purposes in different operations.

Currently, we are already seeing drones being deployed in the Ukraine and Russia War. These drones are fully equipped to function as autonomous weapons, capable of navigating battlefields and attacking targets without any human input. While this might seem astounding to some, these drones represent only the initial phase of AI in warfare.

The militarization of AI will significantly transform warfare and has serious implications for global security. Military capabilities are enhanced by faster data analysis, and AI-powered autonomous weapons enable more precise targeting and operations without human intervention, potentially reducing the risk to soldiers. However, this progress also raises concerns about increased conflict intensity, the possibility of autonomous weapons being hijacked or misused, and the potential for an arms race in AI military technology. Regulating the militarization of AI is fraught with challenges.

Although there is no standardized approach to cyber attacks, states and intergovernmental organizations like NATO have started to outline strategic concepts for cyber warfare to create a framework for when cyber attacks might be utilized. These strategies commonly emphasize both enhancing cyber defense and developing offensive capabilities.

## Case Studies

The FBI warned Congress that Chinese hackers have burrowed deep into the United States' cyber infrastructure in an attempt to cause damage. FBI Director Christopher Wray said Chinese government hackers are targeting water treatment plans, the electrical grid, transportation systems and other critical infrastructure inside the U.S.

Stuart Madnick, an MIT professor of engineering systems and co-founder of Cybersecurity at MIT Sloan (CAMS), has studied and written about the cyber-physical nexus. He said with the widespread arrival of generative AI, concerns about physical attacks being the next phase of cybercrime have grown.

During the Bletchley AI Safety Summit in November 2023, international leaders came together to discuss the vast potential of AI models in promoting economic growth, propelling scientific advances, and providing a wide range of public benefits. They also underscored the security risks that could arise from the irresponsible development and use of AI technologies. The Summit Declaration highlighted the importance of ensuring that AI is designed, developed, deployed, and used in a manner that is safe, human-centric, trustworthy, and responsible for the benefit of all. The NCSC continues to work with international partners and industry to provide guidance on the secure development and use of AI, so that we can realize the benefits that AI offers to society, publishing Guidelines for Secure AI System Development in November 2023.

One of recent memory's biggest and most important cybersecurity events was the Equifax data breach in 2017, which seriously damaged the public's confidence in data security and privacy. Cybercriminals obtained the personal information of about 147 million U.S. citizens without authorisation by exploiting a vulnerability in the Equifax online application.[9] Birth dates, addresses, Social Security numbers, and, in certain situations, driver's license numbers were among the details provided. Following the hack, lawmakers and regulators worldwide demanded tighter data protection regulations and more oversight of the credit reporting sector. In the wake of the incident, the U.S. Congress held hearings. As a condition of the 2018 settlement, Equifax consented to pay up to $700 million in penalties and restitution to the victims of the breach in exchange for cooperating with state attorneys general, the Federal Trade Commission, and the Consumer Financial Protection Bureau. As part of the settlement agreement, Equifax had to undergo regular cybersecurity programme audits and significantly modify its data protocols.

On February 3, the Armed Forces of Lithuania identified a suspicious access to the user account of their distance learning system. Pro-Russian hackers, known as Just Evil, claimed to have infiltrated the military systems of Lithuania and other NATO countries. In a publication in X, Just Evil affirmed that they have hacked the military systems of the United States and the Baltic states, including Lithuania. The National Cybersecurity Center, in active collaboration with the Lithuanian Armed Forces, has begun an investigation, describing the incident as a mid-level cyber incident.

Minneapolis Public Schools informed over 100,000 individuals that their personal information might have been compromised due to a hack earlier this year. On March 7, the Medusa ransomware group claimed responsibility for the attack, demanding $1 million to decrypt the MPS systems. When the school system refused to pay, the group leaked data, including highly sensitive student records, and posted a 51-minute video showing screenshots of the stolen information ten days later. The district explained that they would have alerted victims sooner but needed time to thoroughly examine and identify the sensitive information involved. The breach began on February 6 and continued until February 18, when MPS contacted law enforcement. The district is offering victims 24 months of credit monitoring and identity theft restoration services, along with a dedicated phone line for assistance. Additionally, MPS is reviewing and enhancing its information security policies and procedures, implementing additional protections.

## Bloc Positions

Iran: This country has implemented AI in various fields, such as healthcare, agriculture, finance and in the management of smart cities. Iran has been increasingly active in cyber warfare, leveraging AI and advanced technologies to enhance its cyber capabilities. Notable incidents include the Stuxnet attack on Iran's nuclear facilities, which highlighted the nation's vulnerability and spurred advancements in its cyber capabilities.

North Korea: Notable cyber groups, such as Lazarus Group, have been linked to high-profile cyber incidents, including the Sony Pictures hack (2014) and the WannaCry ransomware attack (2017). North Korea has developed significant capabilities in cyber warfare, leveraging AI and advanced technologies to enhance its offensive and defensive cyber operations.

China: This country has become a global leader in artificial intelligence (AI) and cyber warfare, leveraging its technological advancements to enhance its cyber capabilities. Notable cyber groups, such as APT1, APT10, and APT41, have been linked to various high-profile cyber espionage and cyber theft incidents, including the theft of intellectual property and sensitive government information.

Russia: Russia conducts extensive cyber operations targeting governments, corporations, and critical infrastructure globally. Notable cyber groups, such as APT28 (Fancy Bear) and APT29 (Cozy Bear), have been linked to high-profile cyber espionage and cyberattack incidents, including interference in the 2016 U.S. presidential election and attacks on European countries.

USA: The United States of America is at the spearhead of integrating artificial intelligence into its cyber warfare strategy, taking advantage of advanced technologies to enhance both offensive and defensive cyber capabilities. The U.S conducts sophisticated cyber operations targeting the critical infrastructure, military systems and communication networks of adversaries.

Israel: AI systems in Israel use machine learning to analyze vast amounts of data and detect anomalies that could indicate cyber threats. Units like Unit 8200, Israel's elite cyber intelligence unit, leverage AI for both defensive and offensive cyber operations. This includes intelligence gathering, cyber espionage, and disrupting adversarial networks.

UK: This country, together with various institutions, has managed to develop an offensive and defensive system. The NCSC is the UK's lead organization for cybersecurity. It leverages AI to protect critical infrastructure, government networks, and private sector systems from cyber threats. GCHQ, the UK's intelligence and security organization, uses AI for both defensive and offensive cyber operations. This includes cyber espionage, threat detection, and disrupting adversarial networks. Like these, there are others that work together with the government in defense of the country.

France: ANSSI is France's national cybersecurity agency; nevertheless, it is not the only one. DGSI and DGSE are agencies that use AI for both defensive and offensive cyber operations, including cyber espionage, threat detection, and disrupting adversarial networks. Another one, for example, COMCYBER.

Germany: Germany is actively advancing in the field of AI and integrating these advancements into its cyber defense strategies, as a leading economy in Europe with a strong technological base. The Federal Office for Information Security (BSI) plays a key role in developing and implementing national cybersecurity strategies, incorporating AI to enhance threat detection and response capabilities.

Japan: The National Center of Incident Readiness and Strategy for Cybersecurity (NISC) plays a crucial role in developing and implementing national cybersecurity strategies. Japan actively collaborates with international partners, including the United States and other allies, to enhance collective cybersecurity and address the challenges posed by AI-driven cyber threats.

Canada: As a leader in AI research and innovation, Canada is recognized for its robust advancements in artificial intelligence and its proactive stance in integrating these technologies into cybersecurity frameworks. AI technologies support cyber surveillance operations, including data mining, pattern recognition, and monitoring communications for suspicious activities.

Singapur: The Singaporean government has launched the "National AI Strategy," which aims to position Singapore as a global hub for AI by integrating AI across various sectors, including cybersecurity. Also, The Cyber Security Agency of Singapore (CSA) plays a crucial role in developing and implementing national cybersecurity strategies, incorporating AI to enhance threat detection.

Brazil: The Brazilian government launched the National AI Strategy (Estratégia Brasileira de Inteligência Artificial) in 2021, aiming to promote AI research, development, and adoption across various sectors, including cybersecurity. The Cyber Defense Command (Comando de Defesa Cibernética, CDCiber) plays a crucial role in developing and implementing national cybersecurity strategies, defensive and offensive tools.

Argentina: Argentina is gradually making strides in artificial intelligence (AI) development and is working to integrate these advancements into its cybersecurity strategies. The National Directorate of Cybersecurity (Dirección Nacional de Ciberseguridad) is one of the leading institutions in the development of AI in this country.

Chile: Chile is actively investing in artificial intelligence and integrating these advancements into its cybersecurity framework. In this context, CSIRT, part of the Ministry of Interior and Public Security, is responsible for coordinating cybersecurity efforts across the public and private sectors, leveraging AI to protect critical infrastructure and government networks.

Malaysia: NACSA is Malaysia’s principal agency responsible for cybersecurity, coordinating efforts across government and private sectors to protect critical infrastructure. Also, CyberSecurity Malaysia, this agency under the Ministry of Communications and Multimedia focuses on improving national cybersecurity posture, leveraging AI for threat detection, incident response, and cybersecurity awareness.

UAE: DESC works to protect Dubai's information, communications, and technology infrastructure by incorporating AI for threat detection. TDRA is responsible for regulating the telecommunications sector and ensuring cybersecurity in digital government services. It employs AI to monitor and protect digital infrastructure. Like these, there are various other agencies that work together to optimize the defense and offense mechanisms of the UAE.

Colombia: The Colombian Armed Forces incorporate AI into their cyber defense units to improve the efficiency and effectiveness of military cyber operations and ColCERT is responsible for coordinating responses to cyber incidents, leveraging AI to improve threat detection and response efficiency.

Saudi Arabia: Saudi Federation for Cybersecurity, Programming, and Drones (SAFCSP) promotes cybersecurity awareness, education, and skill development. It uses AI to advance cybersecurity training and simulation exercises. The NCA is responsible for developing and implementing national cybersecurity policies and strategies.

Netherlands: The Dutch Ministry of Defence Cyber Command is responsible for the cyber security of the Netherlands Defence organization and its partners. This plays an important role as the NCSC, which is the body responsible for digital security and cybersecurity in this country.

## Questions A Resolution Must Answer (QARMA's)

1. What role can NATO play in supporting DISEC'S efforts to mitigate the proliferation of AI-based cyber weapons, and how can both entities work together to prevent the rise of AI-driven cyber conflicts into larger crises?

2. How does NATO's strategic framework for the use of artificial intelligence in cyber warfare align with the disarmament, demobilization, and reintegration protocols advocated by the UN Disarmament and International Security Committee?

3. How strict should measures be when it comes to taking action on AI implementation in cybersecurity? Should it be completely prohibited? Should it just be regulated, if so, to what extent?

4. What frameworks should member states implement in order to mitigate the risks associated with AI-enhanced threat technology? Or how can existing cybersecurity measures be adapted to address these threats?

5. How can the international community prevent the escalation of disputes due to AI-driven cyber attacks? How should nations and international bodies address the risks of AI security systems being manipulated or hacked?

6. What role should governments, multinational organizations and industry leaders play in establishing guidelines and standards for the development and deployment of AI as a tool and a threat in cyber warfare? And how should member states adopt international law, standards and treaties to address the proliferation of cyberweapons by AI on a global scale?

## COMMITTEE EXPECTATIONS

We are glad you made it to the end of the study guide!

Always remember that this study guide, as its name states, is just the beginning of your research. We highly encourage you to expand your knowledge and bring new sub-topics to the committee. As a little hint, we suggest researching other implications of AI in cyberwarfare and using previous data to support your knowledge. Also, it is vital to read recent news that may affect the development of the committee, such as the aftermath of COVID-19, the Russia-Ukraine conflict, etc.

Again, if there is anything that is unclear for you, do not hesitate to reach out to any of us! We'll be more than glad to answer your doubts and see you at the conference.

## POSITION DOCUMENT REQUIREMENTS

A Position Paper is a political statement in which delegates analyze and present the opinion of their assigned country on the issue under discussion, focusing on national actions and international affairs of the past and in the development of viable proposals for the topic. Furthermore, a position paper consists of:

- ➔ **Paragraph 1:** Description of the topic's history, without giving an exhaustive account of it, but rather focus on the details that are most important to the delegation's policy.
- ➔ **Paragraph 2:** UN and national policies in plain terms and inclusion of relevant statements, statistics, and research that support the effectiveness of the policy. Comparisons with other global issues are also appropriate here.
- ➔ **Paragraph 3:** Detail of the delegation's proposed solutions to address the topic. Each idea should clearly connect to the specific problem it aims to solve and identify potential obstacles to implementation and how they can be avoided, as a natural extension

Failure to include a bibliography with any position paper will result in instant disqualification and be considered plagiarism. Furthermore, this document has a specific format, which we strongly request delegates to follow otherwise they will not be accepted.

- ➔ Font: Times New Roman 11 pts
- ➔ Line Spacing: 1.15

- ➔ Margins: 2.54 cm from all extremities (standart)
- ➔ Bibliography format: APA 7th edition

Lastly, all position papers are to be delivered by August 16th in PDF format to the following email address: disecpaduamun@gmail.com To ensure no position papers are lost in spam, please send all of them with the subject "Position Paper - Your Country".

**Delegates who do not submit their position papers will NOT be eligible for awards.**

# BIBLIOGRAPHY

*DISEC*. ARC MUN. http://aristoteliocollegemun.weebly.com/disec.html#:~:text=1st%20GA%20%2DDISARMAMENT%20AND%20INTERNATIONAL%20SECURITY%20(DISEC)&text=The%20decisions%20of%201st%20Committee,form%20the%20committee%20for%20DISEC.

United Nations. *UN General Assembly - First Committee - Disarmament and International Security*. https://www.un.org/en/ga/first/.

*Disarmament and International Security Committee – Vancouver Model United Nations*.. https://vmun.com/committees/disec/.

Nigro, P. (2024, 9 january). The intersection of cybersecurity and artificial intelligence. *Security Magazine*. https://www.securitymagazine.com/articles/100312-the-intersection-of-cybersecurity-and-artificial-intelligence#:~:text=In%20the%20late%201990s%20and,might%20indicate%20a%20security%20breach.

SLU, T. T. (2023, 16 octubre). Cyber Security Evolution: AI as a Tool for Attack and Defence. *Telefónica Tech*. https://telefonicatech.com/en/blog/cyber-security-evolution-ai-as-a-tool-for-attack-and-defence.

SITNFlash. (2020, 23 april). *The History of Artificial Intelligence - Science in the News*. Science In The News. https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/.

Bradley, T. (2024, 4 june). AI is the past, present and future of cybersecurity. *Forbes*. https://www.forbes.com/sites/tonybradley/2024/05/17/ai-is-the-past-present-and-future-of-cybersecurity/.

Williams, K. (2024, 3 march). *«Cyber-physical attacks» fueled by AI are a growing threat, experts say*. CNBC. https://www.cnbc.com/2024/03/03/cyber-physical-attacks-fueled-by-ai-are-a-growing-threat-experts-say.html.

*The near-term impact of AI on the cyber threat*. https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat.

Brandefense. (2024, 30 may). *The Impact of Artificial Intelligence on Cyber Warfare*. Brandefense. https://brandefense.io/blog/the-impact-of-artificial-intelligence-on-cyber-warfare/.

Wikipedia contributors. (2024, 8 july). *Lazarus Group*. Wikipedia. https://en.wikipedia.org/wiki/Lazarus_Group

colaboradores de Wikipedia. (2023, 9 december). *Fancy Bear*. Wikipedia, la Enciclopedia Libre. https://es.wikipedia.org/wiki/Fancy_Bear.

Wikipedia contributors. (2024, february 18). *National Cybersecurity Authority (Saudi Arabia)*. Wikipedia. https://en.wikipedia.org/wiki/National_Cybersecurity_Authority_(Saudi_Arabia).

*The near-term impact of AI on the cyber threat*. (s. f.-b). https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat#:~:text=Threat%20actors%2C%20including%20ransomware%20actors,continue%20to%202025%20and%20beyond.