STUDY GUIDE

AI in Cybersecurity and National Security

Examine the use of AI in cyberattacks and cybersecurity defence and discuss potential threats and opportunities in AI-driven warfare and security.

St PETER'S SCHOOL
Barcelona

SMUN 2030

TABLE OF CONTENTS

1. Welcome letter from the Chairs

Greetings, fellow delegates!

It is our pleasure to welcome you to the academic simulation of the United Nations Security Council (UNSC) held in Barcelona by SMUN 2024. In this committee, we gladly present to you a quite broad topic with plenty to discuss: Examining the use of AI in cyberattacks and cybersecurity defence and discussing potential threats and opportunities in AI-driven warfare and security. This should be accompanied by legal aspects which will altogether result in a resolution drawing up regulations and a new convention on cybersecurity and its defence, and AI technology's use within warfare. Please, be aware that this background information in this study guide is only designed to be a starting point for the rest of your independent research, and it is not intended to be a complete guide on the topics. Moreover, this guide cannot, under any circumstances, be used in committee proceedings or used as a primary source of evidence. The more knowledge and insight you have on the agenda, the more you will be capable of influencing the documentation process through committee discussion.

We acknowledge that MUN conferences might be intimidating for first-timers, but it must be made clear that we do not expect the delegates to be highly knowledgeable or articulate. Instead, we're interested in seeing how you can acknowledge discrepancies and different points of view, navigate them, and expand your own foreign policy to address more extensive problems without sacrificing the position of the nation you represent. Essentially, we highly value your creativity and encourage you to come up with ideas that have never been thought of before, or find solutions that were carried out elsewhere and implement these in favour of both topics. We are looking forward to meeting you all soon! Do not be afraid to speak up and be heard. Show your voice, get ready to network, and we wish you all a memorable experience in SMUN 2024!

Kind regards,

Emily, Liza and Ingrid
Chairs of the UN Security Council

2. The United Nations Security Council

The United Nations Security Council, its main characteristics and mandate

The United Nations Security Council (UNSC) is one of the six principal organs of the United Nations (UN) and is charged with ensuring international peace and security, recommending the admission of new UN members to the General Assembly, and approving any changes to the United Nations Charter. Its powers, as outlined in the United Nations Charter, include establishing peacekeeping operations, enacting international sanctions, and authorising military action. The UNSC is the only UN body with authority to issue resolutions that are binding on member states, meaning that all Member States are obligated to comply with Council decisions. The Security Council takes the lead in determining the existence of a threat to the peace or act of aggression, calling upon the parties to a dispute to settle it by peaceful means, and recommends methods of adjustment or terms of settlement.

The UNSC has 15 Member states, each with one vote. The Security Council's five permanent members have the power to veto any substantive resolution, which allows for a permanent member to block the adoption of a resolution, but not to prevent or end a debate. The permanent members of the UNSC are the United States of America, the Russian Federation, the People's Republic of China, the United Kingdom of Great Britain and Northern Ireland, and the French Republic, which were the victorious powers in World War II and have maintained the world's most powerful military forces ever since.

Along with the five permanent members, the Security Council has temporary members that hold their seats on a rotating basis by geographic region. Non-permanent members may be involved in global security briefings. In its first two decades, the Security Council had six non-permanent members, the first of which were the Commonwealth of Australia, the Federal Republic of Brazil, the Arab Republic of Egypt, the United Mexican States, the Kingdom of the Netherlands and the Republic of Poland. In 1965, the number of non-permanent members was expanded to ten. These ten non-permanent members are elected by the United Nations General Assembly for two-year terms starting on January 1st, five members being replaced each year. To be approved, a candidate must receive at least two-thirds of all votes cast for that seat, which can result in a deadlock if there are two roughly evenly matched candidates. A retiring member is not eligible for immediate re-election.

2.1. Veto Power

Under Article 27 of the United Nations Charter, Security Council decisions on all substantive matters require the affirmative votes of three-fifths of the members. A negative vote or a “veto” by a permanent member prevents the adoption of a proposal, even if it has received the required votes. Abstention is not regarded as a veto in most cases, although all five permanent members must vote for adopting any amendment of the UN Charter or any recommendation of the admission of a new UN member state. Procedural matters cannot be vetoed, so the veto right cannot be used to avoid the discussion of an issue. The same holds for certain decisions that directly regard permanent members. Most vetoes have been used in order to block a candidate for Secretary-General, or for the admission of a member state, not in critical international security situations.

2.2. History of the committee

Like the United Nations as a whole, the Security Council was created after World War II to address the failings of the League of Nations, its precedent, in maintaining world peace. It held its first session on January 17th, 1946, but was largely paralyzed in the following decades by the Cold War between the United States and the Soviet Union, along with their respective allies. Nevertheless, the UNSC authorised military interventions in the Korean War and the Congo Crisis, and peacekeeping missions such as those in the Republic of Cyprus, West New Guinea, and the Sinai Peninsula. With the collapse of the Soviet Union, UN peacekeeping efforts increased dramatically in scale, with the Security Council authorising major military and peacekeeping missions in the Republic of Namibia, the Kingdom of Cambodia, the Republic of Bosnia and Herzegovina, the Republic of Rwanda, the Federal Republic of Somalia, the Republic of the Sudan, and the Democratic Republic of the Congo.

2.3. The committee’s mandate

The United Nations Charter established six main organs of the United Nations, including the Security Council. According to the Charter, the United Nations has four purposes:

1. To maintain international peace and security,
2. To develop friendly relations among nations,
3. To cooperate in solving international problems and promoting human rights,
4. And to be a centre for harmonising the actions of nations.

All members of the United Nations agree to accept and carry out the decisions of the Security Council. While other organs of the United Nations make recommendations to member states, only the Security Council has the power to make decisions that member states are then obligated to implement under the Charter.

2.4. Maintaining peace and security

When a complaint concerning a threat to peace is brought before it, the Council's first action is usually to recommend that the parties try to reach agreement by peaceful means. The Council may set forth principles for such an agreement; undertake investigation and mediation, in some cases; dispatch a mission; appoint special envoys; or request the Secretary-General to use his good offices to achieve a pacific settlement of the dispute.

When a dispute leads to hostilities, the Council's primary concern is to bring them to an end as soon as possible. In that case, the Council may issue ceasefire directives that can help prevent an escalation of the conflict; dispatch military observers or a peacekeeping force to help reduce tensions, separate opposing forces and establish a calm in which peaceful settlements may be sought.

Beyond this, the Council may opt for enforcement measures, including economic sanctions, arms embargoes, financial penalties and restrictions, and travel bans; severance of diplomatic relations; blockade; or even collective military action. A chief concern is to focus action on those responsible for the policies or practices condemned by the international community, while minimising the impact of the measures taken on other parts of the population and economy.

2.5. The UNSC's organisation

The Security Council held its first session on 17 January 1946 at Church House, Westminster, London. Since its first meeting, the Security Council has taken permanent residence at the United Nations Headquarters in New York City. It also travelled to many cities, holding sessions in Addis Ababa, Ethiopia, in 1972, in Panama City, Panama, and in Geneva, Switzerland, in 1990. A representative of each of its members must be present at all times at UN Headquarters so that the Security Council can meet at any time as the need arises.

3. Artificial Intelligence

Introduction, its history and its usage in the modern era.

Artificial intelligence (AI) is the intelligence of machines or software, as opposed to the intelligence of humans or animals. It is a field of study in computer science which develops and studies intelligent machines. AI technology is widely used throughout industry, government, and science. For instance, in advanced web search engines (Google Search), recommendation systems, understanding human speech (Siri), self-driving cars, generative and creative tools (ChatGPT) and superhuman play and analysis in strategy games.

The inception of Artificial Intelligence (AI) as a formal field of study can be traced back to the visionary insights of computer scientist John McCarthy, who coined the term in 1955. The ensuing decades have witnessed a captivating journey marked by paradigm shifts, breakthroughs, and challenges.

3.1. Origins of Artificial Intelligence

The formal birth of AI occurred with the Dartmouth Conference in 1956, where McCarthy and fellow researchers congregated to explore the potential of machines emulating human intelligence. Early AI projects focused on symbolic reasoning, laying the foundation for subsequent developments. Allen Newell and Herbert A. Simon's Logic Theorist, conceived in 1955, stands as the inaugural AI program, showcasing the capacity for machines to engage in problem-solving. As AI research progressed, the 1960s and 1970s witnessed the emergence of expert systems designed to replicate human expertise. Pioneering examples such as Dendral and Mycin demonstrated the application of AI in complex problem domains. However, the era also witnessed the onset of an “AI winter” in the 1970s, characterised by scepticism and funding reductions due to unmet expectations and challenges in developing effective AI systems. The 1980s marked a resurgence in AI research, driven by advances in expert systems and knowledge representation. Concurrently, neural networks experienced a revival, with the development of backpropagation as a fundamental training algorithm. Despite these strides, the field faced challenges, and the limitations of expert systems led to a tempered enthusiasm. In the 1990s, machine learning gained prominence, especially in the realms of data mining and pattern recognition.

The 2000s witnessed the rise of machine learning as a dominant paradigm, fueled by advancements in processing power, data storage, and the availability of massive datasets. Notable algorithms, such as support vector machines and decision trees, gained popularity. Symbolising the potential of AI in strategic endeavours, IBM's Deep Blue triumphed over chess champion Garry Kasparov in 1997, illustrating the capacity of machines to excel in complex, cognitive tasks. The past decade ushered in a transformative phase with the ascendancy of deep learning. Neural networks, particularly those with multiple layers, demonstrated unparalleled capabilities in tasks like image recognition and natural language processing. Breakthroughs in the ImageNet competition underscored the potency of deep learning architectures. However, as AI became increasingly integrated into society, concerns related to ethics, bias, and transparency also gained prominence.As we stand at the threshold of the future, the history of AI reflects a dynamic interplay of ambition, innovation, and occasional disillusionment. From the early conceptualizations of machine intelligence to the contemporary era of deep learning, AI has evolved into a pervasive force. The narrative continues, marked by ongoing advancements, ethical considerations, and the imperative of responsible AI development.

3.2. The applications of AI

Healthcare: AI shows promise in enhancing patient care and quality of life. The ethical obligation of medical professionals to employ AI arises when its applications lead to more accurate diagnoses and treatments. AI, acting as a vital tool in medical research, facilitates the processing and integration of Big Data, particularly crucial in organoid and tissue engineering development.

Gaming: AI has been a driving force since the 1950s, showcasing its prowess through notable achievements. From Deep Blue defeating world chess champion Garry Kasparov to AlphaGo's triumph in the complex game of Go, AI has continually pushed the boundaries of what is possible in strategic decision-making.

Military applications: Increasingly prevalent, enhancing command and control, communication, sensors, and autonomous vehicle coordination. AI's role in intelligence collection, logistics, cyber operations, and information operations is shaping modern military strategies.

Generative AI: Exemplified by models like ChatGPT, has gained prominence in the early 2020s. The realistic outputs of AI-based text-to-image generators have sparked widespread attention, even leading to instances of misinformation and fake images. In industry-specific tasks, thousands of successful AI applications address specific challenges across various sectors. Examples range from energy storage and medical diagnosis to military logistics and applications predicting judicial decisions.

Industry Specific Tasks: In agriculture, AI plays a crucial role in optimising farming practices. From identifying irrigation needs to predicting crop ripening times and monitoring soil moisture, AI enhances efficiency and sustainability. The technology is also applied in astronomy, where it aids in the analysis of vast datasets, contributing to the discovery of exoplanets, forecasting solar activity, and distinguishing between signals and instrumental effects in gravitational wave astronomy. Furthermore, AI finds utility in space activities, including space exploration, real-time decision-making for spacecraft, space debris avoidance, and more autonomous space operations.

3.3. The ethics of Artificial Intelligence

AI ethics is a multidisciplinary field that studies how to optimise AI's beneficial impact while reducing risks and adverse outcomes. Examples of AI ethics issues include data responsibility and privacy, fairness, explainability, robustness, transparency, environmental sustainability, inclusion, moral agency, value alignment, accountability, trust, and technology misuse. With the emergence of big data, companies have increased their focus to drive automation and data-driven decision-making across their organisations. While the intention there is usually, if not always, to improve business outcomes, companies are experiencing unforeseen consequences in some of their AI applications, particularly due to poor upfront research design and biassed datasets.

As instances of unfair outcomes have come to light, new guidelines have emerged, primarily from the research and data science communities, to address concerns around the ethics of AI. Leading companies in the field of AI have also taken a vested interest in shaping these guidelines, as they themselves have started to experience some of the consequences for failing to uphold ethical standards within their products. Lack of diligence in this area can result in reputational, regulatory and legal exposure, resulting in costly penalties. As with all technological advances, innovation tends to outpace government regulation in new, emerging fields. As the appropriate expertise develops within the government industry, we

can expect more AI protocols for companies to follow, enabling them to avoid any infringements on human rights and civil liberties.

There are a number of issues that are at the forefront of ethical conversations surrounding AI technologies in the real world. Some of these include:

3.3.1. Foundation models and generative AI

The release of ChatGPT in 2022 marked a true inflection point for artificial intelligence. The abilities of OpenAI's chatbot opened a new constellation of possibilities for what AI can do and how it can be applied across almost all industries. ChatGPT and similar tools are built on foundation models, AI models that can be adapted to a wide range of downstream tasks. Foundation models are typically large-scale generative models, consisting of billions of parameters, that are trained on unlabeled data using self-supervision. This allows foundation models to quickly apply what they've learned in one context to another, making them highly adaptable and able to perform a wide variety of different tasks. Yet there are many potential issues and ethical concerns around foundation models that are commonly recognized in the tech industry, such as bias, generation of false content, lack of explainability, misuse, and societal impact. Many of these issues are relevant to AI in general but take on new urgency in light of the power and availability of foundation models.

3.3.2. Technological singularity

While this topic garners a lot of public attention, many researchers are not concerned with the idea of AI surpassing human intelligence in the near or immediate future. This is also referred to as superintelligence. Despite the fact that Strong AI and superintelligence is not imminent in society, the idea of it raises some interesting questions as we consider the use of autonomous systems, like self-driving cars. It's unrealistic to think that a driverless car would never get into a car accident, but who is responsible and liable under those circumstances? Should we still pursue autonomous vehicles, or do we limit the integration of this technology to create only semi-autonomous vehicles which promote safety among drivers? The jury is still out on this, but these are the types of ethical debates that are occurring as new, innovative AI technology develops.

3.3.3. AI impact on jobs

While a lot of public perception around artificial intelligence centres around job loss, this concern should be probably reframed. With every disruptive, new technology, we see that the market demand for specific job roles shift. For example, when we look at the automotive industry, many manufacturers are shifting to focus on electric vehicle production to align with green initiatives. The energy industry isn't going away, but the source of energy is shifting from a fuel economy to an electric one. Artificial intelligence should be viewed in a similar manner, where artificial intelligence will shift the demand of jobs to other areas. There will need to be individuals to help manage these systems as data grows and changes every day. There will still need to be resources to address more complex problems within the industries that are most likely to be affected by job demand shifts, like customer service. The important aspect of artificial intelligence and its effect on the job market will be helping individuals transition to these new areas of market demand.

3.3.4. Privacy concerns

Privacy tends to be discussed in the context of data privacy, data protection and data security, and these concerns have allowed policymakers to make more strides here in recent years. For example, in 2016, GDPR legislation was created to protect the personal data of people in the European Union and European Economic Area, giving individuals more control of their data. In the United States, individual states are developing policies, such as the California Consumer Privacy Act (CCPA), which require businesses to inform consumers about the collection of their data. This recent legislation has forced companies to rethink how they store and use personally identifiable data (PII). As a result, investments within security have become an increasing priority for businesses as they seek to eliminate any vulnerabilities and opportunities for surveillance, hacking, and cyberattacks.

3.3.5. Bias and discrimination

Instances of bias and discrimination across a number of intelligent systems have raised many ethical questions regarding the use of artificial intelligence. How can we safeguard against bias and discrimination when the training datasets can lend itself to bias? While companies typically have well-meaning intentions around their automation efforts, Reuters journalists highlight some of the unforeseen consequences of incorporating AI into hiring practices. In their effort to automate and simplify a process, Amazon unintentionally biassed potential job candidates by gender for open technical roles, and they ultimately had to scrap

the project. As events like these surface, Harvard Business Review has raised other pointed questions around the use of AI within hiring practices, such as what data should you be able to use when evaluating a candidate for a role. Bias and discrimination aren't limited to the human resources function either; it can be found in a number of applications from facial recognition software to social media algorithms.

3.3.6. Accountability

There is no universal, overarching legislation that regulates AI practices, but many countries and states are working to develop and implement them locally. Some pieces of AI regulation are in place today, with many more forthcoming. To fill the gap, ethical frameworks have emerged as part of a collaboration between ethicists and researchers to govern the construction and distribution of AI models within society. However, at the moment, these only serve to guide, and research shows that the combination of distributed responsibility and lack of foresight into potential consequences isn't necessarily conducive to preventing harm.

3.4. Organisations that promote AI ethics

Since ethical standards are not the primary concern of data engineers and data scientists in the private sector, a number of organisations have emerged to promote ethical conduct in the field of artificial intelligence. For those seeking more information, the following organisations and projects provide resources for enacting AI ethics.

AlgorithmWatch: This non-profit focuses on an explainable and traceable algorithm and decision process in Artificial Intelligence programs.
AI Now Institute: This non-profit at New York University researches AI social implications.
DARPA: The Defense Advanced Research Projects Agency by the US Department of Defense focuses on promoting explainable AI and AI research.
CHAI: The Center for Human-Compatible Artificial Intelligence is a cooperation of various institutes and universities to promote trustworthy AI and provable beneficial systems.
NASCAI: The National Security Commission on Artificial Intelligence is an independent commission that considers the methods and means necessary to advance the development of artificial intelligence, machine learning and associated technologies to comprehensively address the national security and defence needs of the United States.

4. Artificial Intelligence

Artificial Intelligence within security systems in cyberspace.

Cyber Security is the protection of computer systems and networks from attacks by malicious actors that may result in unauthorised information disclosure, theft of, or damage to hardware, software, or data, as well as from the disruption or misdirection of the services they provide. The field is significant due to the expanded reliance on computer systems, the Internet, and wireless network standards such as Bluetooth and Wi-Fi. Also, due to the growth of smart devices, including smartphones, televisions, and the various devices that constitute the Internet of things. Cybersecurity is one of the most significant challenges of the contemporary world, due to both the complexity of information systems and the societies they support. Security is of especially high importance for systems that govern large-scale systems with far-reaching physical effects, such as power distribution, elections, and finance.

4.1. Main threats

With everything turning digital, Cyber Security threats have been growing each day. To prevent cyber threats, it is necessary to analyse all the data and detect any such risks. That is exactly where AI comes in and simplifies this tiresome process of data analysis, data screening and detecting any risks. Cybersecurity comes with its set of unique threats, which include a broad attack surface, hundreds of devices to protect in each organisation, attack vectors that cybercriminals can exploit, a significant shortage of skilled security professionals to handle the growing demands, massive amounts of data that have surpassed human-scale processing capacity, making it a daunting task to analyse and make sense of, amongst others. Moreover, AI in cybersecurity helps prevent threats as well. AI and machine learning are increasingly important for prevention against cybersecurity threats, they can analyse large amounts of data to detect risks like phishing and malware. However, cyber criminals can modify malware code to evade detection. Some more applications of AI in cyber security may be:

1. Breach risk prediction.
2. Phishing detection.
3. Malware detection and prevention.
4. User authentication.

5. Spam filtering.
6. Password protection.
7. Bot identification.
8. Behavioural analysis.
9. Network segmentation and security.
10. Fraud detection.
11. Thread intelligence.
12. Incident response.
13. Vulnerability management.
14. Identity and access management.

4.2. The future of AI in cybersecurity

Artificial intelligence for cyber security has its own advantages as well as disadvantages. On one hand, it improves the analysis, understanding, and prevention of cybercrime, enhancing the trust and safety of companies and customers. However, AI can be resource-intensive and not always practical, and it can also be used by cybercriminals to improve their attacks. The use of AI has been a topic of discussion for some time, with the ability to analyse data quickly being one of the advantages of AI.

5. Artificial Intelligence

Solutions and enforcement of security mechanisms.

5.1. Regulations by international and regional organisations

The existing framework on AI is currently a combination of legal, ethical, and technical guidelines aimed at governing the development, deployment, and use of artificial intelligence. It's important to note that frameworks may vary between countries and organisations.

Several countries have started to implement or consider **national and international regulations** for AI. For instance, the European Union has proposed the *Artificial Intelligence Act*, which aims to regulate AI systems' use and deployment. International organisations such as the OECD (Organization for Economic Co-operation and Development), have

developed guidelines like the *OECD Principles on Artificial Intelligence*, providing a framework for responsible AI development.

Further organisations and institutions have developed **ethical guidelines** to ensure AI is developed and used responsibly, including the IEEE (Institute of Electrical and Electronics Engineers) *Global Initiative on Ethics of Autonomous and Intelligent Systems*, offering a comprehensive set of ethical principles for AI. Industry-specific organisations often create standards to guide the development and deployment of AI technologies within their sectors. These standards aim to address sector-specific challenges and ensure compliance with ethical and legal principles.

Many frameworks emphasise the importance of **transparency** and explainability in AI systems. This involves making AI algorithms understandable and interpretable, especially in critical applications like healthcare, finance, and criminal justice. Norms have also stressed the need for **accountability** when AI systems make decisions. Efforts are being made to mitigate biases in AI algorithms to ensure fair and equitable outcomes. This includes ongoing research on algorithmic bias and discrimination.

Furthermore, considering the data-intensive nature of AI, frameworks often incorporate principles related to **data protection and privacy**. Compliance with existing data protection regulations, such as the GDPR (*General Data Protection Regulation*) in the European Union, is a critical aspect. It is without a doubt that collaboration between governments, industry, academia, and civil society shall be useful for this. Inclusive, multi-stakeholder approaches are seen as essential for addressing the diverse challenges posed by AI.

The UNESCO (United Nations Educational, Scientific and Cultural Organization) has been actively engaged in discussions related to AI ethics. In 2019, UNESCO adopted the *Recommendation on the Ethics of Artificial Intelligence*, which emphasises the **ethical dimensions** of AI, including issues of accountability, transparency, and non-discrimination.

The International Telecommunication Union (ITU), a UN specialised agency for information and communication technologies, has established the *Focus Group on Artificial Intelligence for Autonomous and Assisted Driving*, indicating the UN's interest in the AI applications within specific sectors.

5.2. UN High-Level Panel on Digital Cooperation

The UN Secretary-General's High-Level Panel on Digital Cooperation, established in 2018, released a report in 2019 titled *The Age of Digital Interdependence*, addressing issues related to digital technologies, including AI. The report emphasises the need for global cooperation and the responsible use of technology.

The UN Human Rights Council has addressed the human rights implications of new and emerging technologies, including AI. Discussions within the Human Rights Council have covered topics such as privacy concerns, discrimination, and the impact of Artificial Intelligence on fundamental rights.

While there may not be specific resolutions, these initiatives demonstrate that the United Nations is actively considering the **ethical, social, and human rights** aspects of AI. The field of Artificial Intelligence governance is evolving rapidly, and there may be further developments or resolutions beyond my last update in January 2022. It's advisable to check the latest UN documents and resolutions for the most current information on AI-related initiatives.

6. Bloc Positions

Nations that share similar political interests regarding the topic.

6.1. Western countries

The United States, members of NATO, and other European nations, generally view AI in warfare as both an opportunity and a challenge. On one hand, Artificial Intelligence is a potential force multiplier, enhancing military capabilities across various domains such as intelligence, surveillance, reconnaissance, logistics, and autonomous systems, which is a great advantage for nations in regards to defence and security. Moreover, AI-driven technologies offer the potential for more efficient and effective decision-making processes, including in time-sensitive situations. The negative aspects of AI in warfare according to these countries are the concerns about the ethical implications of using it, particularly regarding autonomous weapons systems and the potential for unintended consequences or escalation, the reliability, safety, and security of AI systems and their susceptibility to hacking, manipulation, or malfunctions.

While Western countries recognise the potential benefits of AI in warfare, they also emphasise the importance of responsible and ethical use, adherence to international law (IL), and maintaining human control over critical military decisions. Although they share similar opinions, there is ongoing discussion within these countries regarding the appropriate balance between leveraging AI for military advantage and mitigating risks associated with its use.

Western countries emphasise the importance of maintaining human oversight and control over AI-driven military operations, particularly in critical decision-making processes. They advocate for international cooperation and the development of a framework to govern the use of AI, including discussions within forums like the United Nations and NATO. Particularly the United States and members of the European Union, are investing heavily in AI research and development for military applications, aiming to maintain technological superiority and address emerging threats. The United States, China, Russia, and some European nations have been investing in AI technologies for various security applications, including cyber defence and military operations. Collaboration between governments, academia, and the private sector is encouraged to advance AI capabilities while addressing ethics and security.

6.1.1. Key nations

The **United States** has a multifaceted view on using AI in warfare, viewing it as a transformative technology with the potential to enhance military capabilities while also recognising the importance of ethical considerations, human oversight, and international cooperation in its development and use in warfare. The U.S. views AI as a critical tool for maintaining military superiority, a strategic advancement including technologies that offer the potential to enhance military capabilities and better operational effectiveness, augmenting human capabilities. Furthemore, the nation has a history of investing significant resources in AI research, development, and adoption for defence applications. Initiatives such as the *Joint Artificial Intelligence* Center (JAIC) aim to accelerate the adoption of AI across the Department of Defense and foster collaboration between government, industry, and academia.

The **United Kingdom** (UK) has a strategic perspective on using AI in warfare that aligns with its broader defence and security objectives, such as it acting as a critical enabler for maintaining military effectiveness and strategic advantage in an evolving security landscape. Similar to other Western countries, the UK prioritises adherence to ethical principles and international legal frameworks in the development and use of AI in warfare, emphasising the

importance of maintaining human oversight and control over critical military decisions, as well as compliance with international humanitarian law (IHL). Initiatives such as the Defence AI Centre and partnerships with tech companies and research institutions demonstrate the UK's commitment to leveraging AI for defence purposes.

Germany has been noted for its distinctive approach to AI in warfare in contrast with other Western countries, particularly concerning its stance on autonomous weapons systems. The German government has expressed concerns about the ethical implications and risks associated with fully autonomous weapons that can make lethal decisions without human intervention. Germany has advocated for international efforts to regulate and ban such weapons, including within the framework of the United Nations. This stance differs from other Western countries, which have not ruled out the possibility of deploying autonomous weapons systems in certain circumstances. In contrast, some Eastern countries have shown greater willingness to explore and develop autonomous weapons systems as part of their military modernization efforts. These countries have expressed fewer reservations about the deployment of such systems, but still emphasise the importance of human intervention.

6.2. Eastern countries

Views on AI in warfare vary among Eastern countries, which include major powers like China and Russia, as well as other nations in the Asia-Pacific region. These nations generally view AI as a critical component of military modernization efforts, with a focus on leveraging technological advancements to enhance military capabilities and address evolving security challenges. These countries are investing in AI research and development to maintain or enhance their military capabilities relative to regional and global rivals.

6.2.1. Key nations

China has emerged as a significant player in AI development and integration into military operations. The Chinese government sees Artificial Intelligence as a key component of its military modernization efforts, aiming to achieve technological parity or superiority with the United States and other Western powers. Chinese military strategy emphasises the importance of AI for enhancing capabilities in areas such as intelligence gathering, command and control, autonomous weapons systems, and unmanned aerial and naval platforms. The nation has invested heavily in its research and development, both within the military and through collaboration with academia and the private sector.

Russia also recognizes the strategic importance of AI in modern warfare and is actively pursuing its integration into military operations. Russian military doctrine highlights the role of AI in information warfare, cyber operations, and autonomous weapon systems. Russian military development efforts focus on leveraging AI for enhancing situational awareness, decision-making processes, and the development of unmanned and autonomous systems for various military applications. Like China, Russia has made significant investments in AI research and development, with an emphasis on maintaining technological parity with Western adversaries.

Other Eastern countries in the Asia-Pacific region, such as **South Korea** and **Japan**, also recognize the importance of AI in warfare and are investing in its development for military applications. These countries are developing AI-driven technologies for intelligence gathering, surveillance, reconnaissance, and the development of unmanned and autonomous systems for military use. These countries are active participants in AI research and development and are increasingly integrating AI capabilities into their defence strategies.

7. Questions and clarifications a resolution must answer

- What alternative approaches or solutions can be incorporated into existing clauses and treaties to improve their effectiveness?
- What are the economic implications for controlling warfare technologies and further innovative systems, such as AI and surveillance?
- How can the international community guarantee and safeguard the wellbeing of politicians, soldiers, and other parties throughout their daily lives?
- Can the use of AI be reduced or controlled equally by any parties?
- To what extent can lethal autonomous weapons be used in warfare?
- Whose responsibility will it be to handle unforeseen consequences?
- To what extent can states be restricted in using defence mechanisms?
- What would be the most effective way to implement existing regulations worldwide?
- Could the international community negotiate the creation of one single regulation?
- What new dispute settlement systems can be implemented to motivate a correct attitude by parties?
- How can compliance with the present global framework be ensured?

Ultimately, this UNSC conference is an opportunity for all participant states to gather and focus on the issues at hand, prevalent in the current world. This negotiation and debate can help us face future challenges including unprecedented wars, riots, and further unwanted violence. As we have seen, current resolutions do not reflect the urgency of the problem of security and defence. At SMUN, our resolution should focus on revamping old beliefs into fresh, relevant clauses. We look forward to your innovative ideas and sincerely encourage creativity and objective thinking.

All the best,

Emily, Liza and Ingrid
Chairs of the UN Security Council

8. Further Reading

Reading and website recommendations to further your knowledge.

Delegates,

We hope you have enjoyed this study guide and the process of furthering your knowledge. However, we leave here some additional links in order for you to continue reading if you wish to do so. As has been previously stated, this study guide is only designed to be a starting point for the rest of your independent research, it is not intended to be a complete guide on the topics. Hence, we attempt to facilitate your research. We hope you enjoy it!

Franke, U. (2019). HARNESSING ARTIFICIAL INTELLIGENCE. European Council on Foreign Relations. http://www.jstor.org/stable/resrep21491

Medeiros, M., & Centre for International Governance Innovation. (2020). Public and Private Dimensions of AI Technology and Security (pp. 20–25). Centre for International Governance Innovation. http://www.jstor.org/stable/resrep27510.6

Antebi, L. (2021). Challenges in Using AI. In Artificial Intelligence and National Security in Israel (pp. 97–112). Institute for National Security Studies. http://www.jstor.org/stable/resrep30590.17

Schmidt, E. (2022). AI, Great Power Competition & National Security. Daedalus, 151(2), 288–298. https://www.jstor.org/stable/48662042

Maymí, F., & Lathrop, S. (2018). AI in Cyberspace: Beyond the Hype. The Cyber Defense Review, 3(3), 71–82. https://www.jstor.org/stable/26554998

9. Citations and references

Kasapoğlu, C., & Kırdemir, B. (2019). WARS OF NONE: ARTIFICIAL INTELLIGENCE AND THE FUTURE OF CONFLICT. Centre for Economics and Foreign Policy Studies. http://www.jstor.org/stable/resrep21050

HUNTER, A. P., SHEPPARD, L. R., KARLÉN, R., & BALIEIRO, L. (2018). CONCEPTUAL FRAMEWORK FOR ARTIFICIAL INTELLIGENCE APPLICATIONS. In ARTIFICIAL INTELLIGENCE AND NATIONAL SECURITY: THE IMPORTANCE OF THE AI ECOSYSTEM (pp. 5–14). Center for Strategic and International Studies (CSIS). http://www.jstor.org/stable/resrep22492.5

What is the Security Council? security council. (n.d.-b). Retrieved from https://www.un.org/securitycouncil/content/what-security-council

Rossi, F. (2018). BUILDING TRUST IN ARTIFICIAL INTELLIGENCE. Journal of International Affairs, 72(1), 127–134. https://www.jstor.org/stable/26588348

Stanley-Lockman, Z., Gilli, A., Gilli, M., & Leonard, A.-S. (2020). Ethical purpose: ethics and values. In “NATO-Mation”: Strategies for Leading in the Age of Artificial Intelligence (pp. 29–34). NATO Defense College. http://www.jstor.org/stable/resrep27711.11

Babuta, A., Oswald, M., & Janjeva, A. (2020). National Security Uses of AI. In Artificial Intelligence and UK National Security: Policy Considerations (pp. 7–20). Royal United Services Institute (RUSI). http://www.jstor.org/stable/resrep40328.7

James Johnson (2019) Artificial intelligence & future warfare: implications for international security, Defense & Security Analysis, 35:2, 147-169, DOI. https://www.tandfonline.com/doi/abs/10.1080/14751798.2019.1600800

Fournier-Tombs, E. (2021). Towards a United Nations Internal Regulation for Artificial Intelligence. Big Data & Society, 8(2). https://doi.org/10.1177/20539517211039493

United Nations Security Council |. (n.d.). https://www.un.org/securitycouncil/

de Almeida, P.G.R., dos Santos, C.D. & Farias, J.S. Artificial Intelligence Regulation: a framework for governance. Ethics Inf Technol 23, 505–525 (2021). https://doi.org/10.1007/s10676-021-09593-z

High-level advisory body on Artificial Intelligence | Office of the secretary-general's Envoy on Technology. (n.d.-a). Retrieved from https://www.un.org/techenvoy/ai-advisory-body

Ai advisory body. (n.d.-a). Retrieved from https://www.un.org/en/ai-advisory-body

Implementation of the UN secretary-general's roadmap on digital cooperation. (2020). https://www.unesco.org/en/articles/implementation-un-secretary-generals-roadmap-digital-cooperation

Araya, D. (2022). Cybersecurity and AI. In Artificial Intelligence for Defence and Security (pp. 13–14). Centre for International Governance Innovation. http://www.jstor.org/stable/resrep42557.11