

JUNIOR ACADEMY MODEL UN X **DISEC** TOPIC GUIDE

> Gaelle Ngabo Hitanshee Sheth

TABLE OF CONTENTS

Letters from Chairs:	
Gaelle Ngabo	1
Hitanshee Sheth	2
Introduction	3
Topic History	5
Current Situation	9
Country Positions	11
Possible Solutions	20
Questions to Consider	22
References	23

JUNIOR ACADEMY MODEL UNITED NATIONS

- Tenth Annual Conference -

JAMUN X SECRETARIAT

Anna Ekmecki Director of Internal Affairs

Brooke Foley Director of Internal Affairs

Claire Jiang Director of Internal Affairs

Katie Cho Director of External Affairs

Suzu Hirai Director of External Affairs

Mia Subrahmanyam Director of External Affairs

Wilber Callejas Director of Operations

Michael Haskell Director of Operations

Kiki Perez Grovas Director of Operations

FACULTY ADVISORS

Mark Kramer Faculty Advisor

Christine Wallace Faculty Advisor What's up, delegates!

Gaelle Ngabo gaenga27@bergen.org

Welcome to JAMUN X! My name is Gaelle Ngabo (she/her), and I am super excited to be your co-chair for this year's DISEC committee! For a bit of background about me, I am a freshman (preferably, freshMUN) in the Academy for Engineering and Design Technology (AEDT), I've been swimming competitively for 6 years, I play the flute, piccolo, and the piano, and I love Robotics. My dream is to be a mechatronic engineer at NASA, which at this rate, will be largely impacted by artificial intelligence. I just started Model UN this year, and I've had some amazing experiences. I am confident this is something I will be doing through high school and possibly through college. But enough about me, whether it's your very first conference, or you're ready to be the next UN Secretary-General, I am super excited about what's in store for all of us.

When deciding a topic, my co-chair and I believed that it was imperative we address the arising concerns when it came to artificial intelligence. This concept has started to gain more attention in recent years. As technology is advancing and new knowledge is being acquired, artificial intelligence is no longer just a website that can do your history essay. It's our generation that is going to experience the benefits – and the downfalls. I can't wait to see what you guys come up with in this committee as we discuss this powerful new technology.

As we debate and discuss, I'm looking for collaboration, inclusion, and intelligent discussion. Model UN isn't just about being the best, it's about working together, building off each other's ideas, and, most importantly, meeting new people and making new friends. As I've traveled to places such as Yale University and Washington, D.C. for conferences, I have had so many fun experiences and met so many amazing people, my personal favorite part of my new Model UN journey. Let's get excited about interesting debates, new experiences, and amazing resolutions. If you have any questions regarding anything, feel free to email me at gaenga27@bergen.org.

With that, I motion to have the best time in this year's JAMUN X DISEC committee! By the chair's discretion, this motion passes!

Can't wait to meet you all :)

Gaelle Ngabo Co-Chair – DISEC gaenga27@bergen.org

JUNIOR ACADEMY MODEL UNITED NATIONS

- Tenth Annual Conference -

JAMUN X SECRETARIAT

Anna Ekmecki Director of Internal Affairs

Brooke Foley Director of Internal Affairs

Claire Jiang Director of Internal Affairs

Katie Cho Director of External Affairs

Suzu Hirai Director of External Affairs

Mia Subrahmanyam Director of External Affairs

Wilber Callejas Director of Operations

Michael Haskell Director of Operations

Kiki Perez Grovas **Director of Operations**

FACULTY ADVISORS

Mark Kramer Faculty Advisor

Christine Wallace Faculty Advisor Hitanshee Sheth hitshe27@bergen.org

Hey Delegates!

My name is Hitanshee Sheth (she/her), and I welcome all of you JAMUN X! I will be your co-chair for DISEC this year, and can't wait to see the unique and well thought ideas that are presented for Weaponization of AI!

As a current freshman in the Academy of Engineering and Design Technology (AEDT), I joined the Model UN family and club this year. I attended multiple committees such as UNODC at Horace Mann, DISEC at Princeton MUN, and CESCR at Yale Model United Nations. Through these experiences, I obtained so much knowledge about international affairs, improved in public speaking, expanded my network of friends that I still stay in touch with, and had so much fun at the same time! The memories created such as late-night dinners, staying up late reviewing opening speeches, the adrenaline rush, and recording everyone's accomplishments throughout the journey are truly special, and long-lasting. As a co-chair, I hope to create the same environment where everyone can push to involve themselves in speaking constantly, creating friendships, and gaining knowledge in various facets of AI in different countries.

My co-chair and I decided on the Weaponization of AI because it is a rising topic in the world that students should be aware of. As technology increases, it isn't just used for educational purposes anymore, but it is also used for harmful actions as well. The reliance on technology has increased, so malware and software attacks can completely obliterate thousands of people's occupations and lifestyles. Furthermore, the integration of artificial intelligence into weaponry creates a potential for autonomous weapons to make life-or-death decisions without human intervention and raises concerns about accountability and the potential for unintended consequences. This is something extremely important that needs to be addressed and actively spoken upon. We both hope to see everyone completely immersed in representing their country, constantly collaborating, and keeping the committee sessions riveting!

Aside from MUN, I am part of Titanium Knights, the school robotics team, where I help build and outreach the robot, and am currently learning how to program in multiple languages. Being a complete music lover, I play the saxophone (2 years) and flute (9 years) [western, and starting to learn the bansuri (Indian flute)], I sing alto for the BCA choir (I have sung Indian classical for 3 years, and been part of choir since 4th grade), and spend my weekends scrolling through Spotify for new songs. So, if you have any great music recommendations, feel free to tell me! I have played various sports such as softball, volleyball, basketball, and tennis, and for the past three years, I have been running and doing track (long distance), and hope to continue it throughout the future. Lastly, I love rewatching my favorite show on Netflix while eating Indo-Chinese food, Suits. So let's all get ready in our suits, formal clothes, and heels, and I can't wait to see you in the committee room. Let's make some AI-mazing memories at JAMUN X!

Hitanshee Sheth Co-Chair – DISEC <u>hitshe27@bergen.org</u>

TOPIC: <u>Weaponization</u> of Artificial <u>Intelligence</u>

INTRODUCTION

The weaponization of AI and technology has become a pressing concern for nations worldwide, encompassing a range of issues from ransomware and malware attacks to using deep fakes and exploiting new technologies for leaking confidential data. These threats not only jeopardize the security and stability of individual nations but also pose a significant risk to global sovereignty. However, addressing these challenges is complicated by the rapid advancement of artificial intelligence, which often advances faster than the development of policies and technologies aimed at protection and defense.

One of the fundamental challenges lies in the inherently human nature of AI's creation and learning process. As AI systems are trained on data generated by humans, they inherit the biases and subjective perspectives inherent in that data. This presents a formidable obstacle in ensuring that AI remains impartial, especially on complex and somewhat controversial topics. Over time, these biases can manifest in the responses that are generated by AI, potentially leading to prejudiced content.

Introduction (Continued)

Moreover, there is an ethical debate presented regarding the use of AI in military weapons, this includes swarm bots, target recognition, AI cybersecurity, etc. As time progresses, this use of AI in the military has continued to be developed and improved, as this is such a new field of military combat. Because of this, the implementation of militarized AI is still an ongoing work in progress. As a result, there were a lot of rising concerns regarding the use of AI in military combat, as some may believe that it is not safe to use novel AI for things such as war in combat, while others believe that this is the next step into revolutionizing the military. This can be a topic debated in this committee.

Addressing the multifaceted challenges posed by AI requires a collaborative and innovative approach. Policymakers, government officials, technologists, and military personnel must work together to develop robust frameworks for regulating AI, ensuring transparency, accountability, and fairness in its deployment. Furthermore, efforts to mitigate bias in AI systems must be prioritized, alongside initiatives to enhance cybersecurity and safeguard privacy rights. Only through concerted action can we harness the transformative potential of AI while minimizing its unintended consequences and safeguarding the interests of society as a whole.

Topic History

Artificial intelligence is arguably the fastest-growing field in this day and age, and it's only growing more rapidly. As more knowledge is being acquired and more forms of AI are being tested, people are starting to become more aware of the massive potential that artificial intelligence has; This awareness is bringing a lot of good to the world. Artificial intelligence is allowing us to know more about weather patterns so we can prepare better for natural disasters, helping us develop custom diagnoses for the sick, automating learning environments, and much more. But with great possibilities, also comes with a lot of potential misuses. Swarm drones, harmful robots, Deep Fakes, and malware attacks are just a few of the many ways that artificial intelligence is being used to harm others. Along with that, as artificial intelligence is getting more and more advanced, we are slowly falling behind when it comes to implementing policies regarding the use of AI, making the use of AI in weapons not exactly illegal. The International Committee of the Red Cross notes that the process by which autonomous weapon systems function raises challenges for compliance with international law and raises ethical concerns for humanity [4].

This highlights that while AI in weapons, swarm drones, military robots, etc. can be useful in some cases, there is also an ethical debate that arises, which should be addressed in this committee as well.

Militarized AI: In 1991, during the Gulf War, the United States military deployed the Patriot Missile Defense System, marking one of the earliest uses of AI in the military. The system utilized AI technology to track and intercept incoming ballistic missiles, distinguishing between friendly and hostile targets in real time [5]. Because artificial intelligence was such a new concept at the time, there were minimal concerns, as this was a baby step in this new realm of technology. This use of AI inspired many nations across the world, sparking an interest in militarized artificial intelligence; Little did people know how far this technology could go. Fast forward to just a few years ago, thousands of AI-enabled "swarm drones" [Photo A] are being considered for use in the Ukraine conflict to overwhelm key strategic Russian targets [2].



Swarm Drones in the Ukranian Military [Photo A]

Topic History

While this was a revolutionary step in the world of the military, this was a very controversial decision. Drone swarms can operate with minimal human intervention, but human intervention with control systems may be necessary for sensitive missions, such as those that could put humans in danger [6]. As time progresses, this use of AI in the military has continued to be developed and improved, as this is such a new field of military combat. Because of this, the implementation of militarized AI is still an ongoing work in progress. As a result, there were a lot of rising concerns regarding the use of AI in military combat. In addition, because this technology is expanding so rapidly, policies are not able to be implemented properly. While the US Department of Defense published a series of policies named "Data, Analytics, and AI Adoption Strategy" a few years ago [7], this is only the case for very few nations. How can we help implement policies for more countries globally, especially those that are less developed? How can we guarantee that AI systems are impartial and do not perpetuate existing biases? How can we ensure that AI decisionmaking mechanisms are transparent? How can we safeguard privacy when AI systems frequently rely on vast data?

How do we get people who understand the technical and regulatory frameworks? Can these implementations pose a risk to the sovereignty of nations? So many questions, and yet, we are still searching for answers. Malware and Data Leaks Using AI: Malware attacks have posed a technological issue long before the use of artificial intelligence, so the issue was only going to get worse once AI was brought into the equation. The first forms of malware were introduced in the early 1970s and were relatively harmless; Small developers would program silly messages to cover over memory in a floppy disk, meaning that all you would see when inserting the disk would be the inputted message rather than your saved data [8]. As technology started to advance, malware attacks started to get more harmful. From the late 1980s to the early 2000s, malware worms were the most popular form of malware. Hackers would hack into software and add worm malware, slowing down computers and making them almost impossible to use. The hackers would then offer to fix the computers for an unreasonable price, and simply remove the inputted virus [8].

<u>Topic History</u> (Continued)

As AI started to become more relevant, the malware started to become more harmful, and would therefore be used for unreasonable ransom. Over the years, AI has greatly strengthened malware attacks, making them more complex and harder to regulate. For example, the Storm Worm could alter its code to dodge antivirus programs. In 2017, WannaCry ransomware utilized AI to swiftly spread across networks, causing widespread damage [9]. Similarly, the Mirai botnet harnessed AI to carry out largescale distributed denial of service (DDoS) attacks in 2016, disrupting internet services [10]. More recently, DeepLocker malware has emerged, using AI to remain hidden until it's ready to strike. These instances highlight the continuous evolution of cyber threats, underscoring the importance of employing AI in defense strategies to counter these sophisticated attacks.

As artificial intelligence is getting more advanced by the day, we need to quickly address these forms of attack and how to stop them before it is too late. AI-Generated Content: Chat GPT, we all love it, and teachers hate it, but there's more to AI-generated content than just software that can give you chemistry answers. Especially more recently, AIgenerated content has become more relevant, and because of how new and upcoming this concept is, there are more flaws than strengths. Music, images, conversations, and videos (also known as deep fakes), are just a few examples of what is currently being generated by artificial intelligence. One of the most pressing dangers of AI-generated content is the spread of misinformation. As AI develops and becomes increasingly sentient-like, we as humans will have trouble differentiating real and fake content from each other [11]. Additionally, as AI-generated deep fakes are becoming more popular, people are starting to use them to attack others. These forms of videos have been used as a form of blackmail, a way to discredit candidates in politics, a way to spread misinformation and fake news, etc. Yes, AI detectors do exist, but they are so newly developed that they are not the most reliable. Another big concern that arises when it comes to AI-generated content is the unavoidable bias.

<u>Topic History</u> (continued)

Because AI uses pre-entered human information to generate content, bias will always be a variable that greatly affects the reliability of anv information that AI generates. An example of this was depicted recently in 2023 when Google was sued for generating content that was biased toward certain races or ethnicities [13]. Users would enter a negative prompt and the AI would explicitly show people of darker skin colors but would generate lighter skin colors once the prompt became more positive [12] [Photo B]. This is an example of pre-entered bias that the AI simply picked up on. Because of how new this concept of AIgenerated content is, we have to be careful about how we use it because so far, the results have not been all successful.

Current Situation

AI weaponization has several effects on a country whether it's through the integration of AI in weaponry, or cyber/malware attacks, data leaks, and perpetuating bias. These actions can affect a country through economic losses, critical infrastructure disruption, national security threats, privacy violations, political instability, and escalation of conflict in general.

For example, recently in February 2024, Russian hackers exploited a bug in a webmail server to inject malware into servers at the embassies and collect information on European and Iranian political and military activities which was part of the espionage campaign.





Google's then new "VisonAI" consistently produced results that pointed towards racial bias [B]

<u>Current</u> <u>Situation(continued)</u>

According to researchers from Recorded Future's Insikt Group, analvzed who attacks and presented this topic at the Munich Security Conference, the goal of this espionage was to obtain strategic advantages against European Security and alliances. These types of attacks pose significant risks to the federal enterprise which means it's a national security threat. [14] In addition to this, since January 2024, Russian state-backed hackers of qained access to some Microsoft's core software systems. They wanted access to "some of the company's source code repositories and internal systems," the tech firm stated in a filing with the US Securities and Exchange Commission. The hackers can use the source code to create followup attacks on other major systems. They had access to unclassified email accounts at the Departments of Homeland Security and Justice. [24]



The debate over AI-controlled weapons has moved along roughly the same lines. There can be malfunctions. or unintended consequences so it is challenging to ensure accountability. However, the development of AI weaponry is still there. Before national security was still skeptical about creating AI weapons and there was no definition universal that was agreed upon. But as time continued, countries started to set aside the ethical, military, and legal aspects and develop more AI weaponry. For example, According to the U.N. report, the Turkish military [20] made Kargu-2 [Photo C1 are fatal autonomous aircraft launched in swarm attacks on behalf of Libya's Government of National Accord against Haftar's militias in March 2021. This marked the first time for a successful attack using AI-equipped drones. The increasing development and use of lethal autonomous systems (LAWS) have led to ethical concerns over the AI weapons race which are amping up tensions militaries and between the possibility of rapid growth by nonstate actors.

<u>Current Situation</u> (continued)

LAWS are a special class of weapon systems that use sensor suites and computer algorithms to independently identify a target and employ a weapon system to destroy it without any human control. Some examples are loitering munitions (exploding drones) and several sentry types of guns. The first documented use of this was during the Libyan War in 2021. [19] They are mostly used to patrol areas and divebomb at enemy radar signals '. While LAWS is still largely unnoticed, (SALWs) Small arms and light weapons contributed to almost half of all deaths between 2010 and 2015. They are also easier to obtain, and in thev are used empowering authoritarian governments, militias. terrorist gangs, and organizations. Although these weapons are easier to create, the service and optimization of these procedures in weapons manufacturing of SALWs do contribute to harm, and the effect of AI on these industries is not well known. [19]

The opposing side of the large debate on whether artificial Intelligence should be integrated into militarization is due to the fact that it can be used for resourceful aspects of war. AI is used in combat simulation and training and has been used especially in the U.S. Army for a noticeable period of time.

It consists of systems engineering, software engineering. and computer science in order to create digital models that prepare soldiers with combat systems utilized during operations. Sentient Digital has recently developed a naval wargaming simulation that leverages LLM (large language model) together with ACI (application-centric infrastructure) architecture.It creates realistic scenarios that generate communication similar to real-life adversaries.

Let alone AI used for wars on land, but using it in space is the Militarization of AI at a larger scale and level. The weaponization of space with AI-controlled weapons raises concerns about the risks of accidental or intentional collisions between satellites, and the escalation of conflict in the Earth's atmosphere. As countries continue to develop and deploy AI technologies for military purposes, including in space, there is а need for enhanced international cooperation, transparency, and dialogue to address the complex challenges and risks associated with the militarization of AI in space. Currently, the biggest threats to the WGS (Wideband Global Satcom), which are high-capacity communicators for the warfighters nation's through control systems, are China and Russia. Both these nations have ground-based anti-satellite weapons that have the potential to destroy other satellites in low earth orbit. These two countries have also launched cyber attacks against U.S. and NATO-affiliated satellites. [15]

Current Situation(continued)

In recent years, GPS systems and the information collected from satellites and the Air Force are heavily relied on during warfare. So, it makes sense for countries to start to take advantage of the fact that it is now possible to travel into space and take warfare to another level. President Trump announced on June 18, 2018, the creation of a new military branch, the Space Force. In addition to this, the Pentagon, which is the headquarters building of the United States Department of Defense, planned for the new branch. [15]

In the current generation, as social media is a rising platform for business, and a mode of communication, consequently the biggest rise in identity fraud rate at 274% was between 2021 and 2023. [16]



As AI continues to advance, deep fakes are becoming increasingly more popular – especially amongst politicians. Deep fakes are produced by extracting parts of someone's face or voice and slowly compiling them into one frame [D].

Country Policies

North America

North America stands as the leading continent in artificial intelligence, due to its pivotal role in research, development, and organization, with both opportunities and challenges. The continent is home to some of the world's most influential AI research institutions, tech companies, and talent pools, making it a global powerhouse in AI innovation. Silicon Valley in the United States, particularly, serves as a beacon of AI excellence, attracting top researchers, entrepreneurs, and investors from around the world. Leading tech giants like Google, Microsoft, and Facebook have heavily invested in AI development, research and propelling breakthroughs in deep learning, natural language processing, and computer vision. Moreover, North American startups are trailblazing AI-driven solutions across diverse industries, including healthcare. finance. transportation, and entertainment, fueling economic growth and innovation.

Leaning towards the governmental aspect, AI deep fakes raise election risks and spread misinformation that can cause havoc to billions of people. There have been multiple events of feigning a voice or generating fake videos of political leaders. In 2024, a video of late Indonesian President Suharto advocating for the political party he once supported went viral. In addition to this, in the U.S. New Hampshire voters heard a deep fake of President Joe Biden asking them not to vote in the presidential primary. A 3rd example of this was a planted deep fake of former Pakistani prime minister Imran Khan announcing that his party was boycotting them. [17] According to reports, at least 60 countries and more than 4 billion people will be voting for their leaders, and 2024 is set up to be the biggest global election year in history, so deep fakes have become a major concern worldwide [Photo D].

<u>Country Policies (continued)</u>

However, amidst these advancements, challenges such as ethical considerations surrounding AI deployment, including privacy, bias, and algorithmic transparency, persist. Additionally, concerns about job displacement and inequality due to automation and AI adoption raise socio-economic challenges that get attention. Despite this, North America's expertise and leadership in AI innovation present immense opportunities for driving technological advancement and shaping the future of AI on a global scale.

United States

The delegation of the United States has continuously been developing more advanced technology every second. This country has been a global leader in responsible military use of AI and autonomy, and we can see this through recent events. In November 2023, the State Department's press release stated a groundbreaking initiative containing 10 concrete measures to guide the responsible development and use of military applications of AI and autonomy. In addition to that, the Defense Department published a series of policies on military AI and autonomy called the Data, Analytics, and AI Adoption Strategy on November 2nd. These policies included making sure that minimized unintended bias in military AI capabilities, overseeing the usage of AI weaponry, users are aware of the capabilities, data sources, and design procedures, and ensuring transparency. [35] The US has supported Ukraine in the current war against Russia by using piloted surveillance tracking soldiers' fitness, predicting when Air Force planes need maintenance, and constantly receiving information on rivals in space. In addition to this, the Pentagon officials and industry experts believe that within the next few years, the U.S. will have developed fully autonomous lethal weapons, (LAWS). [36] In terms of cybercrime, the US has several limitations that make it hard for solutions to overcome malware and software attacks that result in hundreds of billions of dollars in losses and threaten public safety and economic security. For example, the U.S. Marshals Service reported in February that it had been a victim of a ransomware attack where hackers opened sensitive files which included information about investigative targets and workers' data. To fix these problems, in 2022, Congress required the Department of Justice to develop a specific department for the FBI's National Incident-Based Reporting systems. This department will start to collect reports on crime from law enforcement across the country and this can help give law enforcement the tools they need to collect complete and accurate data on cybercrime to help address this worldwide issue. [37]

Canada

Canadian Armed Forces (CAF) and AI systems are finding limited operational and business applications within the Canadian Military establishment not only for technical reasons, but also due to the historical, cultural, and organizational aspects. However, study shows that in the future AI technologies will continue to be developed in the Department of National Defence and Canadian Armed Forces. [38] The military is on the verge of adopting artificial intelligence and in late 2023, Defence Minister Bill Blair stated that Canada will recognize the importance of AI in the military and make sure the expansion of AI in the military domain will be done responsibly. In 2022, the CAF improved military data and technology systems by releasing the Digital Campaign Plan and this plan promised that the Armed forces will be "digitally transformed" by 2030. [39]

Europe

Europe is the hub for technological innovation and research with leading tech companies and institutions. Currently, most investments are happening in the fields of AI, biotechnology, and renewable energy. Europe has been making steady progress in the field of AI in the aspects of research and development. The countries are constantly investing in AI education, gaining more partnerships on AI research which allows for a larger pool of money and resources to develop AI devices rapidly, in addition to this, Europe regulates and has various rules to prevent misuse of this fresh technology. This continent is proficient in overcoming obstacles and challenges related to the militarization of AI in European countries. For example, this region faces various security challenges which include cyber threats, and terrorism which impels the need for advanced military capabilities and cooperation between the countries and NATO allies. On March 13th, 2024, the European Union adopted the Artificial Intelligence Act which aimed to regulate AI technologies and ensure responsible and ethical use of it. It included rules on user transparency, accountability, high-risk applications, unintended bias, autonomous vehicles, and weapons.

France

The delegation of France is actively investing in the development and deployment of AIpowered weaponry as a part of its national defense strategy. France has been involving itself in public debate and dialogue on the ethical and security implications of AIpowered weaponry involving policymakers, military experts, academics, and civil society organizations. The President of the Republic adopted the National Strategy for AI in November 2021 as a part of the French "2030 plan". The national AI strategy aims to expand the pool of AI-trained talents, and this plan enhances the nation's skills and establishes France as a leader in embedded AI and trustworthy AI. [41]

United Kingdom

In June 2022, the UK's Ministry of Defence (MOD) released the Defence Artificial Intelligence Strategy along with the policy statement Ambitious, Safe, Responsible: Our approach to the delivery of AI-enabled capability in Defence. By releasing this they hope to transform the MOD into an 'AI Ready' organization, be able to adapt and exploit AI at a certain pace so they have a better defense advantage and have the upper hand, strengthening the UK: defense, security, stability, and democratic values. [39] In addition to this, the British Prime Minister Sunak led the UK AI Safety Summit where UK leaders gathered senior government officials from major AI companies which resulted in a joint commitment. They announced the new UK-based AI safety institute and a major push to support regular, scientist-led assessments of AI functions and safety risks. [40] The Summit's progress was a huge diplomatic achievement, the UK had brought in the EU, United States, China, India, and other major countries to sign the agreement. The United Kingdom's focus on AI safety and ethics reflects its commitment to ensuring that AI technologies are developed and used responsibly. The initiatives that the UK takes show the strategic approach to harnessing the potential of AI for defense and security purposes.

<u>Asia</u>

Asia stands as one of the leading continents when it comes to AI advancement, characterized by diverse economies and cultures that contribute to a diverse spectrum of AI research, development, and deployment. Across the continent, there is rapid growth towards AI adoption, with significant investments in research, infrastructure, and talent development. Notably, Asia's collective efforts in AI address region-specific challenges such as urbanization, aging populations, and environmental sustainability, with initiatives ranging from smart cities to healthcare optimization [27]. The continent is demonstrating how to use AI for the benefit of all, rather than using it for harm or personal gain, an approach that all nations should look up to.

<u>China</u>

The delegation of China has been aggressively pursuing AI development as part of its broader strategy to become a global leader in technology. The Chinese government has made substantial investments through ambitious plans and substantial investments in research, development, and deployment. With the unveiling of its "New Generation Artificial Intelligence Development Plan" in 2017 [28], China outlined its vision to become the world's primary AI innovation center by 2030, emphasizing technology development, talent cultivation, and ecosystem creation. The government's strong support and funding for AI initiatives, coupled with the leadership of prominent technology companies like Alibaba, Tencent, and Baidu, have propelled China to the forefront of AI innovation. Leveraging its vast population and data resources, China has made significant strides in AI technologies such as facial recognition, natural language processing, and recommendation systems. While prioritizing AI development, China has also addressed ethical concerns and regulatory challenges through the issuance of guidelines and regulations. Additionally, China actively collaborates with international partners to promote global collaboration and address common challenges in the AI field, positioning itself as a key player in shaping the future of artificial intelligence.

<u>Singapore</u>

The delegation of Singapore has positioned itself as a regional hub for artificial intelligence (AI) innovation and adoption, backed by government support, advanced infrastructure, and strategic initiatives. To become a Smart Nation, Singapore has invested significantly in AI research, development, and deployment across various sectors. The government's National AI Strategy [29], introduced in 2019, underscores Singapore's commitment to harnessing AI for economic growth and societal advancement. Singapore boasts a vibrant AI ecosystem comprising research institutions, companies, multinational corporations, and government agencies, supported by robust digital infrastructure and favorable regulatory frameworks. Industries in Singapore, including finance, healthcare, logistics, and transportation, are increasingly embracing AI technologies to drive productivity and competitiveness. The country prioritizes talent development in AI-related fields through scholarships, grants, and training programs, fostering a skilled workforce in AI research and data science. Furthermore, Singapore addresses ethical considerations and regulatory challenges through guidelines and frameworks to promote responsible AI innovation, data privacy, and cybersecurity, positioning itself as a leader in responsible and impactful AI adoption.

Middle East

In the Middle East, governments are actively embracing artificial intelligence as a driver of economic growth and societal advancement. National strategies and initiatives prioritize AI development, fostering innovation hubs, and sectoral adoption. AI is transforming industries such as healthcare, finance, and transportation, enhancing efficiency and service delivery. Moreover, investments in education and training programs are equipping individuals with AI skills, positioning the region for future job opportunities. However, alongside the benefits, challenges persist. Ethical concerns around algorithmic bias and privacy must be addressed while ensuring data accessibility and quality is crucial for AI deployment. Strengthening cybersecurity measures and harmonizing regulatory frameworks will further support responsible AI adoption [30]. By tackling these challenges, the Middle East can unlock AI's full potential, driving inclusive and sustainable development in the region.

Saudi Arabia

The delegation of Saudi Arabia has emerged as a significant player in artificial intelligence, demonstrating substantial advancements and investments in research, development, and adoption. Anchored by its Vision 2030, the country has prioritized AI as a cornerstone of economic diversification and technological progress. The implementation of a National AI Strategy underscores its commitment to fostering innovation and collaboration across sectors. Saudi Arabia's investments in AI research, partnerships with global technology leaders, and initiatives like the Saudi Data and Artificial Intelligence Authority (SDAIA) reflect its proactive approach to AI development [31]. This has resulted in notable sectoral adoption, particularly in healthcare, finance, and education, where AI technologies are enhancing efficiency and driving innovation. Despite some challenges including a large skill gap and rising ethical debate, Saudi Arabia's positive trajectory in AI positions it as a key player in shaping the future of AI innovation and deployment in the region and beyond [31].

<u>Israel</u>

The delegation of Israel has established a good name for itself in the world of artificial intelligence, celebrated for its flourishing ecosystem of tech companies, research institutions, and talent in AI-related fields, even in the midst of geopolitical conflict. With a strong emphasis on innovation and entrepreneurship, Israel has cultivated a dynamic AI landscape that attracts investment and collaboration from around the world. The country's robust infrastructure, supportive government policies, and vibrant techcompany culture have contributed to its success in AI development and adoption. Israeli companies are forming AI solutions across various areas, including cybersecurity, healthcare, autonomous vehicles, and fintech, driving innovation and economic growth. Additionally, Israel's world-class research institutions, such as the Technion-Israel Institute of Technology and the Weizmann Institute of Science, are at the forefront of AI research [32], contributing to breakthroughs in machine learning, computer vision, and natural language processing. However, challenges such as addressing ethical concerns, ensuring diversity and inclusivity in AI development, and mitigating the potential for algorithmic bias remain. With that being said, Israel's position in AI is predominantly positive, characterized by innovation, collaboration, and a commitment to leveraging AI for societal and economic advancement.

Africa

Both opportunities and challenges characterize Africa's position in artificial intelligence. On the positive side, the continent is experiencing a growing interest and investment in AI technologies, driven by its potential to address various socio-economic challenges and drive innovation. African countries are increasingly recognizing AI as a tool for economic development, with initiatives such as the African Union's "AI for Africa" strategy aiming to leverage AI for sustainable development. Furthermore, Africa is home to a burgeoning tech startup ecosystem, with hubs emerging in countries like Nigeria, Kenya, and South Africa, fostering innovation and entrepreneurship in AI. Several African companies are developing AI-powered solutions tailored to the continent's unique needs, including healthcare diagnostics, agriculture optimization, and financial inclusion. However, challenges such as limited access to data, inadequate infrastructure, and a shortage of AI talent hinder the continent's progress in AI adoption and development. Additionally, there are concerns about the potential for AI to exacerbate existing inequalities and biases if not deployed responsibly. Despite these challenges, Africa's position in AI is characterized by a growing momentum towards leveraging technology for positive impact, with opportunities for collaboration and innovation to drive inclusive growth and development across the continent.

South Africa

The delegation of South Africa's position in artificial intelligence is marked by both progress and challenges. The country has made significant strides in AI research, development, and adoption, fueled by a growing interest in leveraging technology for economic growth and social development. South Africa is home to several leading research institutions and universities with expertise in AI, such as the University of Cape Town and the Council for Scientific and Industrial Research (CSIR), which contribute to advancements in AI technology and innovation. Additionally, South African startups and companies are increasingly exploring AI-driven solutions across various sectors, including healthcare, finance, agriculture, and education, to address local challenges and drive efficiency. Initiatives like the South African Center for Artificial Intelligence Research (CAIR) and the South African National AI Strategy [33] aim to foster collaboration, skills development, and innovation in AI. However, challenges such as limited access to data, infrastructure constraints, and a shortage of AI talent pose obstacles to the country's AI ambitions. Additionally, concerns about ethical considerations, including bias and fairness in AI algorithms, remain pertinent. That being said, South Africa's commitment to advancing AI technologies holds promise for driving inclusive growth and societal impact in the country and beyond.

Nigeria

The delegation of Nigeria's stance on artificial intelligence reflects a dynamic mix of innovation and entrepreneurship, with significant strides made in recent years. Nigeria takes advantage of its flourishing economy and has implemented thriving tech companies, particularly in cities like Lagos and Abuja, where entrepreneurs are leveraging AI to address local challenges and drive economic growth [34]. The country's youthful population and vibrant tech community contribute to a strong foundation for AI innovation, with companies developing AI-powered solutions in areas such as healthcare, agriculture, fintech, and education. Furthermore, Nigeria is home to leading AI research institutions and initiatives, such as the African Institute for Mathematical Sciences (AIMS) and the Nigerian AI Hub, which foster collaboration, skills development, and knowledge sharing in AI [34]. However, challenges such as infrastructure constraints, limited access to data, and a shortage of AI talent hinder the country's AI ambitions. Additionally, concerns about ethical considerations, including bias and fairness in AI algorithms, remain pertinent. Despite these challenges, Nigeria's burgeoning AI ecosystem holds promise for driving inclusive growth and societal impact, positioning the country as a key player in the African AI landscape.

Possible Solutions

The Commonwealth has yet to come up with a proper legal system to enforce the utilization of technology in the right way. One main issue with this is that certain countries are more ready for AI development than others. A potential solution to this problem is creating a scale to determine the security of said country's AI platform, based on said country's past AI research.

In addition to scale, another potential solution should be in regards to educating the people and underdeveloped countries about transparency, user privacy, the risks and harms of AI, and how to fix problems if a malware or software attack. For example, using AI to save time with mundane tasks like laundry or washing dishes is something that everyone would benefit from, and workplaces could use AI to enable faster data processing and allow for more developments. Additionally, learning how to work around malware dysfunctions and hackers is another central issue that the public must be educated on. Users should learn to differentiate between fake and real viruses, learn how the AI infrastructure works, and how to react to malware and ransom attacks.

To get rid of unintended bias, some ways to tackle this would be to foster diversity and to bring different perspectives and experiences to the development and testing of AI systems. Bias awareness training could also spread information and fairness to AI developers, scientists, and other stakeholders involved in the development and deployment of AI systems.

Possible Solutions

There could also be some type of user feedback so not only government officials help out, but there is a variety of opinions on what the bias level is.

In regards to AI weaponry, establishing clear regulations and standards for all countries and delegations would regulate the ethical use of AI-powered weaponry. There should be regulations regarding solving humanitarian crises if an unmanned consequence were to happen. Implementing safeguards, controls, and mitigation regulations that stop potential misuse, and ensure compliance with international humanitarian law, ethical principles, and regulations. Having transparency between the common people and the weapon holders would ensure some level of trust, awareness of consequences, and responsible use of AI technologies.

Addressing malware and software attacks requires a proactive, adaptive, and comprehensive strategy and approach that will help prevent, detect, and recover regulations. There should be continuous and constant monitoring, logging, and analysis of systems and data to detect and identify dangerous or suspicious activities. Similar to education, there should be some sort of training in regards to cyber security which practices safe computing habits, spreading awareness, recognizing, and reporting

Questions to Consider

- 1.How can we implement artificial intelligence in certain nations while preserving national sovereignty?
- 2.How do we prevent unintended consequences or malfunctions of AI systems in the military?
- 3.How does the increase of AI-enabled weapons impact strategic stability and arms control in the military?
- 4. How can we ensure transparency and accountability in the use of AI technologies by specific organizations?
- 5.What strategies can organizations adopt to protect themselves from artificial intelligence-formed ransomware attacks?
- 6.How can biases in generative AI models be identified, quantified, and mitigated?

a.Is it even possible?

7. Are current laws and regulations sufficient to address the evolving threats posed by harmful AI?

a. If not, how can this be addressed?

8. What responsibility do developers and organizations have in promoting fairness and equity in generative AI content?

https://unu.edu/article/militarization_ai_has_severe_implications_global_security_and_warfare [1]

https://www.forbes.com/sites/forbestechcouncil/2024/03/08/navigating-the-risks-of-aiweaponization/?sh=71c5fb7e7f07[2]

https://www.frontiersin.org/articles/10.3389/frai.2023.1154184/full [3]

https://www.citizen.org/article/ai-joereport/#:~:text=Summarizing%20the%20key%20ethical%20issues,compliance%20with%20inte rnational%20law%2C%20including [4]

https://www.brookings.edu/articles/understanding-the-errors-introduced-by-military-aiapplications/

[5]

<u>https://www.gao.gov/products/gao_23_</u> 106930#:~:text=of%20drone%20swarms-,Challenges,could%20put%20humans%20in%20dang <u>er</u>. [6]

https://www.defense.gov/News/News-Stories/Article/Article/3597093/us-endorsesresponsible-ai-measures-for-global-militaries/ [7]

https://www.ibm.com/blog/malware-history/[8]

https://www.england.nhs.uk/long-read/case-study-wannacry-attack/[9]

https://www.malwarebytes.com/what-was-the-mirai-botnet [10]

https://medium.com/@jacobemil.heldt/the-dangers-of-ai-generated-content-3078e08f6fad [11]

https://www.euronews.com/next/2024/03/09/ai-models-found-to-show-language-bias-byrecommending-black-defendents-be-sentenced-to-dea [12]

https://fortune.com/2022/03/19/not_googly_enough_google_sued_by_black_ex_employee_ over-racially_blased_culture_april_curley_san_diego_alaphabet_inc/ [13]

https://therecord.media/russia-aligned-hackers-target-european-and-iranian-embassiescyber-espionage [14]

https://www.defenseone.com/insights/cards/space-based-c4isr/8/?oref=d1-cards-cardstacktoc [15]

https://www.cnbc.com/2024/03/14/as-asia-enters-a-deepfake-era-is-it-ready-to-handleelection-interference.html [16]

https://www.npr.org/2024/02/08/1229641751/ai-deepfakes-election-risks-lawmakers-techcompanies-artificial-intelligence [17]

https://sdi.ai/blog/the-most-useful-military-applications-ofai/#:~:text=It%20combines%20systems%20engineering%20%20software,in%20order%20to% 20train%20soldiers.[18]

https://montrealethics.ai/the-evolution-of-war-how-ai-has-changed-military-weaponry-andtechnology/ [19]

https://www.washingtonpost.com/technology/2021/07/07/ai-weapons-us-military/[20]

https://www.theatlantic.com/ideas/archive/2024/02/artificial-intelligence-war-autonomousweapons/677306/[21]

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10030838/#:~:text=Lethal%20autonomous%20 weapons%20and%20AWS,drone%20swarms%20with%20autonomous%20targeting [22]

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10030838/ [23]

https://www.cnn.com/2024/03/08/tech/microsoft-russia-hack/index.html [24]

https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents [25]

https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systemsmaurer.htm [26]

https://www.brookings.edu/articles/ai-in-the-global-south-opportunities-and-challengestowards-more-inclusive-governance/[27]

https://digichina.stanford.edu/work/full_translation_chinas_new_generation_artificial_ intelligence_development_plan_2017/[28]

https://www.smartnation.gov.sg/nais/ [29]

https://www.bloomberg.com/news/articles/2024-04-11/race-for-ai-supremacy-in-middleeast-is-measured-in-data-centers [30]

https://www.defenseone.com/insights/cards/space-based-c4isr/8/?oref=d1-cards-cardstacktoc[15]

https://www.cnbc.com/2024/03/14/as-asia-enters-a-deepfake-era-is-it-ready-to-handleelection-interference.html [16]

https://www.npr.org/2024/02/08/1229641751/ai-deepfakes-election-risks-lawmakers-techcompanies-artificial-intelligence [17]

https://sdi.ai/blog/the-most-useful-military-applications-ofai/#:~:text=It%20combines%20systems%20engineering%20%20software,in%20order%20to% 20train%20soldiers.[18]

https://montrealethics.ai/the-evolution-of-war-how-ai-has-changed-military-weaponry-andtechnology/[19]

https://www.washingtonpost.com/technology/2021/07/07/ai-weapons-us-military/[20]

https://www.theatlantic.com/ideas/archive/2024/02/artificial-intelligence-war-autonomousweapons/677306/ [21]

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10030838/#:~:text=Lethal%20autonomous%20 weapons%20and%20AWS,drone%20swarms%20with%20autonomous%20targeting [22]

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10030838/[23]

https://www.cnn.com/2024/03/08/tech/microsoft-russia-hack/index.html[24]

https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents [25]

https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systemsmaurer.htm [26]

https://www.brookings.edu/articles/ai-in-the-global-south-opportunities-and-challengestowards-more-inclusive-governance/[27]

https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificialintelligence-development-plan-2017/[28]

https://www.smartnation.gov.sg/nais/ [29]

https://www.bloomberg.com/news/articles/2024-04-11/race-for-ai-supremacy-in-middleeast-is-measured-in-data-centers [30]

https://www.saudiembassy.net/vision-2030 [31]

https://allenai.org/ai2-israel [32]

https://www.michalsons.com/blog/south-africas-national-aiplan/72988#:~:text=Through%20strategic%20initiatives%20and%20a,delivery%2C%20and%20 ensure%20sustainable%20development. [33]

https://guardian.ng/news/minister-unveils-artificial-intelligence-hub-in-lagos/[34]

https://www.defense.gov/News/News-Stories/Article/Article/3597093/us-endorsesresponsible-ai-measures-for-globalmilitaries/#:~:text=%22The%20United%20States%20has%20been,declaration%20builds%20on %20these%20efforts.[35]

https://apnews.com/article/us-military-ai-projects-0773b4937801e7a0573f44b57a9a5942 [36]

https://www.gao.gov/blog/u.s.-less-prepared-fight-cybercrime-it-could-be [37]

https://defence.ai/studies-reports/defence-ai-canada/ [38]

https://mcmillan.ca/insights/publications/fusing-ai-with-national-defence-department-ofnational-defence-finalizing-ai-

strategy/#:-:text=In%20a%20statement%20in%20late,military%20domain%20is%20done%20r esponsibly. [39]

https://carnegieendowment.org/2023/11/09/uk-ai-safety-summit-opened-new-chapter-in-aidiplomacy-pub-90968 [40]

https://digital_skills_jobs.europa.eu/en/actions/national_initiatives/national_strategies/france_ national_strategy_ ai#:~:text=The%20strategy%20supports%20the%20growth,of%20AI%20into%20the%20econ omy [41]