Security Council

Topic A: “Assessing the implications of AI technologies for international security due to probable access to personal information and data bases.”

UNDERSECRETARY: Mariana Gascón

MODERATOR: Natalia Gascón

CHAIR: Maika Fernández

CFMUN

CFMUN

Welcoming letter

Dear delegates,

Welcome to this edition of Colegio Fontanar Model of the United Nations. We are very excited to have you at the Security Council, thank you for choosing this committee.

We will focus on the implications of Artificial Intelligence technologies for international security, and Nuclear Non-Proliferation, where we will assess the effectiveness of existing treaties in preventing the spread of nuclear weapons.

We look forward to engage in thoughtful discussions on how to address these pressing challenges. We wish you all the best in your preparations and in your participation throughout this model.

Sincerely,
Natalia Gascón and Maika Fernández
Moderator and Chair of Security Council

Table of contents

I. Committee Background

II. Introduction to the Topic

III. Evolution of the Topic

IV. Relevant Events
A. Panorama
B. Points of View

V. UN and External Actions

VI. Conclusion

VII. Committee Focus

VIII. Participation List

IX. References

I. Committee Background

The Security Council is one of the six main organs of the United Nations.
It has the responsibility of maintaining international peace and security, and determining threats to the peace or acts of aggression. The committee must solve problems by peaceful means, help reach agreements, recommend methods of adjustment, impose sanctions or even use the force to restore peace and security.

It was created in 1945, however, it took its first session in London on January 17th, 1946.
The Security Council has 15 members, 5 permanent (The United States, China, France, Russia and The United Kingdom) and 10 non-permanent members.
Also it has established actions such as UN political missions and development of peacekeeping operations.

II. Introduction to the Topic

The rapid development of Artificial Intelligence (AI) technologies present, both, opportunities and risks for international security, particularly regarding the access and misuse of personal information and databases.

AI, which involves systems that perform tasks requiring human-like intelligence, is transforming various sectors, including defense, healthcare, and finance. However, the integration of AI raises concerns about privacy violations, cyber-attacks, and the potential data breaches.

While AI can enhance national security by supporting cyber-defense and counter-terrorism efforts, it also poses threats such as espionage, disinformation, and hacking.

The ethical and legal challenges of AI's access to sensitive data further complicate the situation.

II. Introduction to the Topic

As AI continues to evolve, it is crucial for the global community, particularly the UN Security Council, to develop frameworks to regulate its use and mitigate its risks, while also fostering innovation and maintaining international peace and security.

III. Evolution of the Topic

The relationship between Artificial Intelligence (AI) and international security has evolved as AI capabilities have grown and expanded into various sectors.

Initially, AI was mainly focused on research and specific applications, with limited security implications. Over time, as AI systems advanced, they began being integrated into cybersecurity, military defense, and intelligence operations, helping to predict threats and track suspicious activities.

As AI's ability to analyze and process large volumes of data increased, concerns about privacy and data misuse also grew.

Malicious actors began using AI for cyber-attacks, identity theft, and disinformation, which raised alarms about its potential use to disrupt national security and global stability.

III. Evolution of the Topic

These developments highlighted the need for regulations and ethical frameworks to govern AI usage, particularly regarding autonomous systems and data protection.

The UN and other international bodies began focusing on how to balance AI's benefits with security and privacy concerns, but the rapid pace of technological progress continues to challenge global efforts to keep up with regulation.

As AI continues to evolve with new technologies like deep learning and quantum computing, the risks and implications for international security continue to grow, making it essential for nations to cooperate on creating effective governance and protective measures.

IV. Relevant Events

A. Panorama

- Early Development of AI (1950s-1960s):

Initial AI research laid the foundation for future applications in military and intelligence, initially it had almost not direct security impact.

- Rise of Cybersecurity (1990s-2000s):

AI began to play a role in cybersecurity, helping to detect cyber threats and protecting national security infrastructure.

- Stuxnet Cyberattack (2010):

The Stuxnet virus demonstrated how AI-driven algorithms could be used for cyber-conflicts, highlighting the risks of AI in national security.

- Autonomous Weapons Development (2010s):

The development of AI-powered autonomous weapons raised ethical and security concerns about accountability and military use.

IV. Relevant Events

- Cambridge Analytica Scandal (2018):

AI-driven data mining and surveillance were used to manipulate elections, raising alarms about AI's potency for political interference and privacy violations.

- UN Reports on AI and Security (2020s):

The UN began focusing on global AI regulations, addressing ethical concerns in military and security applications.

- AI-Driven Cyberattacks (2020s):

Increased AI-powered cyberattacks targeted critical infrastructure, highlighting the necessity of stronger defenses against AI threats.

- AI Governance Initiatives (2021-Present):

Countries began developing national AI strategies and regulatory frameworks to manage AI's ethical use, while the UN continues calling for global cooperation on AI governance.

IV. Relevant Events

- Autonomous Systems in Global Security (Ongoing):

The growing integration of AI in military and surveillance systems underscores the need for international regulations to ensure ethical use and secure development.

B. Points of View

United States: The U.S. prioritizes AI in national security, investing in military technologies of this type, and addressing AI-related risks, such as cyberattacks.

China: China has integrated AI into its national strategy, especially for military and surveillance uses, sparking global security concerns.

V. UN and External Actions

UN ACTIONS:

- UN Group of Governmental Experts (GGE) on Cybersecurity: Focused on international law's application to AI in cybersecurity, promotes global norms for accountability in AI-driven cyberattacks.
- UN Office for Disarmament Affairs (ODA): Addresses the risks of autonomous weapons and the need of a regulation of AI in military technology to comply with international law.
- UNESCO's AI Ethics Recommendation: Developed a global framework to ensure AI is used responsibly, with a focus on privacy, equity, and human rights.
- UN Security Council and AI Discussions: While AI hasn't been directly addressed in resolutions, the Security Council has discussed cybersecurity and the security risks posed by AI.

V. UN and External Actions

- AI Governance Proposals: The UN has been advocating for international frameworks for AI governance, emphasizing ethical use, privacy, and the prevention of misuse in surveillance.

EXTERNAL ACTIONS:

- European Union's AI Regulation Framework: The EU introduced the Artificial Intelligence Act, aiming to regulate AI by risk level and ensuring transparency, accountability, and data protection.
- Private Sector Contributions: Technological important companies, like Google and Microsoft collaborate on ethical AI development, while NGOs like Access Now and EFF advocate for responsible AI use in security and privacy.

V. UN and External Actions

- AI for Good Global Summit (ITU): The ITU's summit promotes AI development for global public good, including ethical considerations related to privacy and security.
- Global Partnership on AI (GPAI): An initiative promoting responsible AI development, with a focus on ensuring AI in security is ethical and compliant with international law.

VI. Conclusion

The rise of AI technologies poses significant challenges for international security, especially regarding access to personal data and the potential misuse in areas like surveillance and cyberattacks.

While the UN has made important efforts through initiatives like the Group of Governmental Experts on Cybersecurity and UNESCO's AI ethics recommendations, global cooperation and regulatory frameworks are still developing. External actions, including national regulations and private sector initiatives, have made a progress, but remain incomplete.

Addressing these risks requires a coordinated global effort to ensure that AI is used responsibly and ethically.

It is essential to establish clear norms and regulations to protect privacy, safeguard human rights, and prevent security threats.

VI. Conclusion

The importance of solving this issue lies in ensuring that AI technologies contribute to global security, rather than exacerbating existing risks in a rapidly evolving digital landscape.

VII. Committee Focus

- How can the international community establish clear ethical guidelines for AI technologies to balance national security concerns with the protection of individual privacy?
- What international frameworks or agreements should be developed to regulate the use of AI in military field and surveillance technologies to prevent misuse or escalation of conflicts?
- In what ways can technological companies collaborate to ensure that AI systems are transparent, accountable, and secure against cyberattacks or unauthorized access to personal data?
- What role should the United Nations play in fostering global cooperation to create a multilateral approach for addressing AI's impact on international security and privacy?

VII. Committee Focus

- How can AI technologies be used proactively to enhance cybersecurity and prevent digital threats, while ensuring that such technologies do not compromise human rights or civil liberties?

VIII. Participation List

- Arab Republic of Egypt
- Canada
- Commonwealth of Australia
- Co-operative Republic of Guyana
- Democratic People's Republic of Korea
- French Republic
- Islamic Republic of Iran
- Japan
- Kingdom of Sweden
- People's Democratic Republic of Algeria
- People's Republic of China
- Republic of Ecuador
- Republic of Malta
- Republic of Mozambique
- Republic of Sierra Leone
- Republic of Slovenia
- Russian Federation
- Swiss Confederation
- United Kingdom of Great Britain and Northern Ireland
- United States of America

IX. References

Almeida, V., & Gasser, U. (2019). *The need for international cooperation on AI governance.* Recovered from: https://www.brookings.edu

Amnesty International. (2020). *Artificial intelligence and human rights: A guide for governments, business, and civil society.* Recovered from: https://www.amnesty.org

Binns, R. (2018). *On the ethics of artificial intelligence. AI & Society.* Recovered from: https://doi.org/10.1007/s00146-018-0812-4

European Commission. (2021). *Artificial Intelligence Act: Proposal for a Regulation on Artificial Intelligence.* Recovered from: https://ec.europa.eu/digital-strategy/our-policies/artificial-intelligence_en

Floridi. L. (2018). *AI and the ethical use of personal data: The foundation of responsible AI governance. Journal of Information Ethics.* Recovered from: https://doi.org/10.3143/jie.27.1.61

GGE (Group of Governmental Experts on Cybersecurity). (2019). *The need for international cooperation on AI governance.* Recovered from: https://www.un.org

IX. References

International Telecommunication Union (ITU). (2020). *AI for good: Ensuring ethical artificial intelligence development*. Recovered from: https://www.itu.int

Jouan, L. (2020). *Artificial intelligence in military operations: International security and arms control. International Affairs Review*. Recovered from: https://www.iar.org

North Korea. (2015). *Center for Arms Control and Non-Proliferation*. Recovered from: https://armscontrolcenter.org/countries/north-korea/

UNESCO. (2021). *Recommendation on the ethics of artificial intelligence*. Recovered from: https://www.unesco.org

United Nations. (2021). *Artificial Intelligence and Its Impact on International Security and Governance*. Recovered from: https://www.un.org