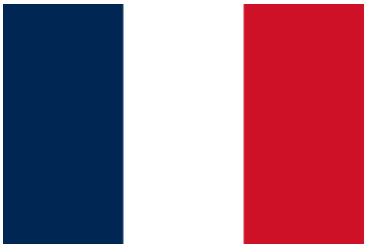
Document
Example

Position Paper

Gimnazija Bežigrad Model United Nations

Written By: Polina Kaspranova

Committee: Human Rights Council
Delegation: République française (French Republic)
Delegate: Polina Kaspranova
Topics: A) Enhancing cybersecurity measures to protect critical Infrastructure from cyber threats during conflicts
B) The potential impact of AI on international security and potential worldwide regulation of its excesses



A) Enhancing cybersecurity measures to protect critical infrastructure from cyber threats during conflicts

The French Republic has for some time recognized the importance of the digital world and with it the impact of cyber operations in conflicts as well as cyber security in general. As the leading power in cyber security globally, ranking 9th at the Global Cybersecurity Index in 2020, our nation is well equipped to lead the efforts towards a more secure digital future. As the digital realm becomes increasingly integral to modern politics, the need for robust cybersecurity measures is indispensable. France stands resolute in addressing the multifaceted challenges posed by cyber operations during conflicts and acknowledges the importance of collaborative international initiatives to ensure a secure digital future.

In our view, the first step towards protecting critical infrastructure from cyber threats during conflicts starts from a legal perspective. We believe that first and foremost we must identify perpetrators and differentiate cybercrime from cyber warfare. France acknowledges the challenges in attributing cyber attacks to their perpetrators, given the anonymity afforded by the digital realm. We emphasize the necessity of developing a robust legal framework to enable states to identify and hold accountable those responsible for cyber attacks. Effective attribution is crucial to deterring malicious actors and ensuring accountability.

In line with this commitment, France is actively investing in the development of cybersecurity capabilities. Our nation boasts a skilled workforce of cybersecurity professionals, the French government has invested in training programs, encouraging professionals and students to pursue careers in cybersecurity, and we are committed to further nurturing talent in this field. For instance, institutions like the National Institute for Research in Computer Science and Automation (INRIA) collaborate with universities to offer advanced courses in cybersecurity.

We recognize the need for international cooperation in capacity-building programs, especially for developing nations, to bolster their cybersecurity defences. The French government supports capacity-building programs in developing nations through collaborations with international organizations such as the United Nations and the European Union.

Moreover, France acknowledges the blurring line between cybercrime and cyber warfare and supports the establishment of clear criteria to differentiate between the two. This understanding is vital for shaping appropriate responses to cyber attacks. We endorse international capacity-building programs to enhance the cybersecurity capabilities of nations, fostering cooperation to address the challenges posed by cyber operations in ongoing conflicts.

In the opinion of France, while it is crucial to protect critical infrastructure from cyber threats during conflicts, we must first strive to prevent such attacks in the first place, which is why it is of the outmost importance to our nation to begin our efforts in identifying the roots of the problem and working on fighting them first and foremost. We recognize that it is in everyone's benefit and interest, for governments to work alongside private companies, such as Microsoft and Google, in identifying perpetrators behind cyber operations. The National Cybersecurity Agency of France (ANSSI) works closely with private companies to share threat intelligence

and improve overall cybersecurity resilience. This collaborative approach ensures a coordinated response to emerging cyber threats. However, we share concerns about potential bias and disproportionate information sharing, influenced by the governments of host countries. To address this, we propose the creation of an independent United Nations Office for Cyber Security (UNOCS).

UNOCS would have the authority and resources to conduct fact-finding missions, identify perpetrators, and ensure unbiased access to relevant data. Alternatively, the office could collaborate with private companies, compelling them to comply with requests to access pertinent data. France acknowledges the complexity of these negotiation but believes this approach would be the most efficient in achieving the desired transparency.

Finally, France supports the idea of developing a universal metric to determine whether a cyber operation constitutes an act of war. This metric, based on factors such as material damage denominated in currency and affected sectors, would provide a standardized assessment. France encourages and participates in collaborative efforts to establish a universally accepted metric, fostering transparency and predictability in responses to cyber incidents. Such metric is yet another step to preventing cyber-attacks, as it allows us to define what constitutes as an attack, what constitutes as an act of war, and what a crime. This will furtherly allow us to implement changes in our legal systems, defining clear consequences for actions, as todays laws on punishment of those committing such crimes are in our opinion, too blurry.

In conclusion, the French Republic stands at the forefront of promoting international cybersecurity efforts. Our commitment to building cybersecurity capabilities, fostering international cooperation, and advocating for an independent UNOCS, as well as a universal metric, reflects our dedication to ensure a safer and more prosperous digital future for all nations. France urges fellow member states to join hands in addressing the critical issue of enhancing cybersecurity measures during conflicts for the collective well-being of the international community. If the committee will vote in favour of the establishment of such body, we wow to continue not working within it, but also in partnership with our allies in the European Union, NATO, and others. France is strongly committed to coming closer to a resolution of cyberwarfare in partnership with our allies.

B) The potential impact of AI on international security and potential worldwide regulation of its excesses

The advent of Artificial Intelligence (AI) presents both unprecedented opportunities and challenges, particularly in the realm of international security. The French republic feels strongly on the issue, and I more than committed to ensuring global peace and security despite many threats, such as artificial intelligence. We advocate for regulation and comprehensive worldwide regulation to address its excesses.

Recent data indicates a substantial 30% increase in global AI expenditures over the last two years. This surge underscores the widespread integration of AI technologies, including within the sphere of defence and security. The implications of this rapid development necessitate a closer examination of its potential impact on the international security landscape. The growing sophistication of AI technologies introduces novel threats, ranging from cybersecurity vulnerabilities to the development of autonomous weapon systems. These challenges transcend national borders, emphasizing the need for collective and pre-emptive measures to ensure responsible AI deployment and mitigate potential risks.

From the French perspective, the rapid advancement of Artificial Intelligence (AI) poses a multifaceted threat to international security, necessitating urgent global attention and regulation. The exponential increase in global AI expenditures, notably within defense and security sectors, underscores the pressing need for comprehensive measures. France recognizes that the growing sophistication of AI technologies introduces novel challenges, ranging from cybersecurity vulnerabilities to the development of autonomous weapon systems.

These threats extend beyond national borders, emphasizing the imperative for collective action to address the potential risks associated with AI. The intricate nature of AI's impact on international security demands a nuanced response, considering the potential for misuse, unintended consequences, and the erosion of traditional security paradigms. France is deeply concerned about the potential for AI to be exploited for malicious purposes in cyber warfare, undermining the stability of nations and exacerbating global tensions.

In response to these challenges, France actively advocates for the establishment of international norms governing the responsible use of AI in security contexts. This includes maintaining human control over AI systems, prohibiting the development of autonomous weapons, and implementing safeguards to prevent the malevolent use of AI in cyber operations. We have already invested over 1.5 billion euros into AI research and development, and we encourage other UN member states to do the same. Only together can we tackle what poses a global threat. We believe that tackling a problem, no matter of which magnitude, must begin with understand it. This, our investment into AI research reaffirms our commitment to understand Artificial Intelligence, and at the same time, fostering innovation while prioritizing ethical and responsible AI development.

Recognizing the inherently cross-border nature of AI challenges, France advocates for the establishment of a dedicated multilateral forum, potentially under the auspices of the United Nations. This forum would serve as a platform for information-sharing, the exchange of best practices, and the development of common standards to address the diverse dimensions of AI in the realm of international security.

France proposes the formulation of international norms governing the responsible use of AI in security contexts. These norms should encompass principles such as maintaining human control over AI systems, prohibiting the development of autonomous weapon systems, and implementing safeguards against the malicious use of AI for cyber warfare. As part of our commitment to working side by side with other member states, we are actively participating in collaborative research initiatives with international partners to explore the dual-use potential of AI technologies. These initiatives aim to better understand the risks and benefits associated with AI in security contexts and facilitate the development of informed policies.

On the national front, the French government is establishing research centres dedicated to AI ethics, fostering innovation, and ensuring a robust regulatory framework to govern AI applications in defence and security. France emphasizes the importance of upholding fundamental human rights in the development and deployment of AI technologies. Any regulatory framework must include provisions to prevent the misuse of AI in ways that could compromise individual liberties and privacy.

Finally, the French Republic recognizes the transformative potential of AI in bolstering global security measures. However, we also acknowledge the responsibility to prevent and mitigate potential risks associated with its use. Through collaborative efforts, including the establishment of international norms and forums for cooperation, we can harness the benefits of AI while safeguarding international security.

France stands ready to engage in constructive dialogue with fellow Security Council members to ensure a comprehensive and effective approach to the regulation of AI and its impact on global security. Together, we can build a future where AI serves as a force for good, advancing security and prosperity for all nations.