GLOBSEC
IDEAS SHAPING THE WORLD

Government of the Netherlands

REAIM
Responsible AI in the Military domain

AI in the Realm of War: Defence Roundtable

“Artificial intelligence is a technology that fundamentally influences our world, from everyday life to high tech processes in the military domain. Yet, apart from benefits connected to this game changing technology, we must also pay close attention to potential risks.

I am therefore grateful to GLOBSEC for organizing a highly topical roundtable discussion focusing on the AI in the realm of war. An event that served as a kick-off session to the Global ministerial conference on responsible military development, application and use of artificial intelligence, which will be coordinated by the Kingdom of the Netherlands in February 2023.

The upcoming high-level event which will address one of key priorities of the Dutch government and its Special Envoy Ed Kronenburg, will follow one ambition - launching a joint international action for the responsible use of AI, thus framing this important agenda for the months to come.”

H.E. Gabriella Sancisi, Ambassador of the Kingdom of the Netherlands to Slovakia

Exclusive discussion hosted by GLOBSEC and the Embassy of the Kingdom of the Netherlands

Date: October 17th 2022

Time: 14:30 – 16:00 CET

Venue: GLOBSEC Headquarters, myhive Tower II, Vajnorská 100/B, Bratislava

Speakers:

Professor **Jean-Marc Rickli**, Head of Global and Emerging Risk, Geneva Centre for Security Policy

Eric Richardson, International lawyer, administrative and regulatory specialist

Led by: **Roger Hilton**, GLOBSEC Defence Fellow

This discussion was organised as part of REAIM 2023, a global summit that the Dutch Minister of Foreign Affairs will organise in cooperation with the Dutch Ministry of Defence in February 2023. REAIM 2023 aims to create a platform for a multistakeholder approach to take place regarding opportunities and challenges in the ever-widening implementation of AI, particularly in the military field. The summit will offer the possibility for various parties to share insights and exchange ideas, spread awareness on the importance and the advantages of the use of AI, as well as identify risks and their respective mitigation. The ideal scenario would see the establishment of global cooperation mechanisms and common responsible approaches. The October 17th roundtable was a chance to test out early ideas on the subject, engage in constructive debate, and provide some pragmatic guidance in the lead up the 2023 Summit.

Global cooperation for responsible AI use as part of the political agenda

AI technologies are increasingly playing a role in ongoing international conflicts. From Eastern Europe to the Caucasus, these technologies have assumed a leading role on the battlefield with no signs of exhaustion.

Other influential factors in theatre operations have been the “information and disinformation strategies” conducted via social media which have contributed to building narratives seeking to discredit or reinforce belligerent sides. As it relates to AI, its specific application to distort images and spread fake news used to destabilise troops’ morale and manipulate the wider public is an underappreciated feature that requires further scrutiny.

When it comes to the use of AI, the primary areas to review include but are limited to **its research and application, the identification of risks, and their mitigation through the adoption of common codes of conduct and a regulatory framework**.

From a global regulatory angle, Europe remains a consumer rather than a significant R&D contributor in the uses and implementation of AI technologies. Yet, it has widespread regulatory experience that could be better strategically deployed. Discussion on regulations would be incomplete without industrial base partners who continue to drive innovation. There are also country-wide AI strategies, as well as academic, business, and civil society approaches that already exist or are being developed that could be useful to a global AI debate.

Looking at Ukraine and CEE, what can be done next in the region?

The war in Ukraine has introduced the concept of “information dominance” as Open Source Intelligence (OSINT) has seen its important role progressively increase in the dynamics on the ground. Furthermore, a significant amount of data showing targets and positions has surfaced online through social media. Russia has a strong disinformation strategy, but Ukraine has unexpectedly responded due to their information sphere dominance.

What are the government’s options when approaching the world of AI?

Governments should have a ‘safe course’ and a regulatory approach to the accessibility of lethal AI technologies aspects that could profoundly impact battlefield situations. For this reason, there is a strong chance that segments of a developing technology will be highly regulated or even banned outside of the military realm. Four major risks of this include:

Accidents – instances in which AI is responsible for the loss of human lives and how it can be explained. AI might also act in unexpected and unsafe behaviour.

Loss of human control – humans have the ability to de-escalate and choose not to engage. In contrast, AI and algorithms do not necessarily work in a broader context that would enable such decision-making.

Explaining what is happening – the devil is in the data. The reason for which something occurred will be hidden in the details of big data that is fed to the machine learning algorithm.

Intentional misuse – most smart technologies’ weakest link is the human factor. There exist situations in which the human factor could decide to manipulate, abuse, or outright sabotage AI systems.

The implementation of existing technological applications such as ‘swarming’ or autonomous lethal decision-making should not be taken without strong considerations for ethical and moral responsibilities. Indeed, the international community should agree upon limitations and standards connected to their use.

What role should the private sector play?

Militaries do not want to have their weapons unaccounted for, and once there is an established line of code, it will be impossible to stop the proliferation. To avoid commercial technology being weaponised with malicious purposes, the costs of these technologies should be inaccessible through high market entry costs and the presence of kill switches.

Collaboration among private sector actors should also be established as they not only have access to the technology but to big data as well.

US and China do not want to be involved in any possible regulatory framework. What would be the features of these possible protocols or treaties?

Building an ethical and responsible framework in which AI can operate is complex. Industries' codes of conduct and special agreements to avoid targeting civilians' critical infrastructures in war zones can pave the way for a better environment and a safer development and deployment of AI technologies.

Takeaways for consideration:

- *For responsible use of AI technologies, policymakers must be aware of their functions, limits, and risks related to their use. Knowing the risks makes it possible to find ways to mitigate their effects.*
- *US and China haven't opted for a regulatory approach when it comes to the use of AI in the military domain, and since the EU currently stands way behind in the research, development, and deployment of these technologies, possible regulation might hinder this process.*
- *Global coordination for the responsible use of AI might be a utopic scenario. Cooperation will most likely develop at the regional level first, while also considering the division between democracies and authoritarian regimes.*

Policy Rapporteurs:

Juraj Kuruc, Fellow and Project Manager, Future of Security Programme

Federica Mangiameli, Project Assistant

Catherine Girard, Communications Manager