Ensuring Our Competitive Edge

May 2018

THE CASE FOR A TRANSATLANTIC AI CENTRE OF EXCELLENCE

James Townsend, Alena Kudzko, Tomáš A. Nagy

This policy paper constitutes the first in a series of publications developed within the framework of the GLOBSEC Artificial Intelligence for Security Initiative (G-AIS), GLOBSEC´s flagship project examining the impact of transformative technology on the transatlantic defence and security policy. GLOBSEC is fully independent in implementing the project and has editorial responsibility for all views and opinions expressed herein.

Our generation is **standing on the edge of a historical change** in one particular element of the nature of warfare – the role of human beings in its conduct. The ability of the transatlantic community to explore, control, utilise and mitigate the phenomenon of Artificial Intelligence (AI) to its comparative advantage might easily constitute the key aspect of maintaining its geopolitical pre-eminence. We believe that a conceptual and ambitious attempt to understand the implications and tap the positive potential of AI should commence with the establishment of an expertise boosting platform – or as we call it, the ***Transatlantic Centre of Excellence for Artificial Intelligence (CoE)***.

Our call to establish the CoE stems from and aims to further build upon the intellectual groundwork laid out by the **GLOBSEC NATO Adaptation Initiative**. Chaired by General John R. Allen and ably assisted by a team of academics, diplomats and military personnel with over 250 years accumulated experience, the Initiative recommended that, in order to adapt to the new reality, the Alliance should.

Establish New Centres of Excellence: A bespoke Hyper War Centre of Excellence would help generate a coherent approach to future war, and combine the work on Artificial Intelligence and expanded NATO cyber defence. NATO urgently needs a coherent approach to the development and application of artificial intelligence (AI) and its family of capabilities to defence and deterrence. Such a Centre would necessarily need to train and educate NATO's civilian and military leadership, and include staff courses for NATO international personnel and member nation civilians. Such a centre would also afford the Alliance opportunities for industry-partnership in this area of revolutionary technologies.

Each generation in recent history has had the privilege to witness a transformation of warfare, governance and profound shift in the way **humanity perceives (in)security as a direct result of technological and scientific advancement**. The early 20th century brought us chemical weapons and the ability to mass-deploy lethal tools.

The mid-20th century witnessed the rise of machinery empowered individuals on the battlefield with automated weapons. The dawn of the Cold War brought the ascent of nuclear power and the threat of mass destruction.

In the 21st Century, as Artificial Intelligence (AI) has gradually become one of the key defining features of global technological advancement, its continuous functional establishment in a broad spectrum of areas - ranging from global finance to the defence industry to essentially every piece of software-based electronic appliance - will alter our understanding of the limits of defensive platforms, reform the modality of governance and challenge our perception of (in)security. AI-related trends will have **profound and increasing implications for the global security landscape**. It will force government agencies to increase the pace of procurement processes, enhance and expand private sector expertise, and integrate R&D processes across the hardware-software board of development.

More and more actors have started to acknowledge the salience of AI and its multifaceted impact on security and defence. We laud this effort. But at a time when the rules for international cooperation are being unravelled by rising revisionists, coordination and alignment with allies is prerequisite for meeting the challenges of our fast-changing world.

Why the transatlantic community needs a CoE for AI?

The rationale for the establishment of the CoE rests on several arguments:

1. *"For everything to remain the same, everything must change."* For NATO to maintain its strategic global leadership in an age of technology-driven and technology-altered threats, its military, strategic, and organisational set-up must be adjusted. One cannot address new threats with old blueprints, nor can one fight new wars with old weapons and tactics.

   Developing sufficient operational readiness to address the AI phenomenon is dependent on efficient institutional adaptability. Technological progress should be supplemented with organisational and doctrinal change covering a spectrum of issues from weapons and procurement to intelligence sharing, decision-making and training of personnel. The *Center of Excellence* for AI would significantly help to **raise political capital, prioritise precious budgetary resources and stimulate institutional reforms** by increasing the understanding of AI´s nature, complexity and potential.

2. The transatlantic community is behind the curve of 21st century conflict, with its current and potential **adversaries, most prominently Russia and China, already endorsing** the prospects of utilising technological trends to change the global balance of power to their interest. To avoid a strategic surprise, Allies need to enhance collective effort.

3. With global players elevating their AI efforts, fears of a contemporary arms race are well-founded. However, the **CoE is not about imprudently accelerating an AI arms race. On the contrary, it should help to manage and control this phenomenon**. Bolstered cooperation among Allies would help introduce multilateral rules of AI utilisation in the security domain to avoid harmful consequences.

4. Technology (including AI) constitutes immense potential to empower **smaller- and non-state actors** in their pursuit of (il)legitimate security objectives. Moreover, with the myriad possibilities that AI introduces – faster decision-making, automation, greater digital anonymity, more complicated accountability – **new threats** emerge and traditional threats (of terrorism, inter-state warfare, WMD proliferation) receive an "AI-upgrade". The Alliance has no choice but to factor into its strategies and responses these new threats and adversaries.

5. While the efforts of individual Allies to grasp the beneficial and dangerous potential of AI is commendable, uncoordinated, uneven and unaligned efforts within the Alliance can be detrimental to its success. **The risks posed by a multi-speed and non-interoperable Alliance are too real.** Concerns about the increasing capability gap and lack of inter-operability go far beyond equipment and weaponry and extend to intelligence gathering, data analysis, foresight, operational structures, and personnel qualifications.

6. **A lack of attention to AI in the context of hybrid warfare can debilitate the Alliance by diminishing and destroying trust.** With AI increasingly capable of producing audio and video spoofs that are barely distinguishable from authentic materials – not to mention attacking and infiltrating communication channels - reality loses its anchors and trust is hard to maintain. In addition, decision-making slows down, while automated simultaneous attacks in multiple domains require immediate reaction. Expertise on how to address issues pertaining to cooperation and decision-making can only be developed in-house.

7. Major breakthroughs in AI have so far largely been developed by the globalised private sector. Effective national security policies might rest on a state's ability to reach out to the global marketplace as well as strengthening cooperation with allies to expand talent and innovation. However, **coordinating cross-border industrial partnerships on a larger scale** would allow investment into a wider range of projects. The latest trend of shielding cutting-edge technologies vital for national security from foreign investment and control further amplifies the need for a CoE. Cooperation between Allies through a CoE would mitigate the downsides of the inward-looking approach to R&D and help ensure progress through maintaining the availability of R&D to partners.

8. With the US as global leader and countries like France and the UK able to provide needed investment and large data sets to spearhead AI development, **small states are at risk of falling behind**. The pooling of resources that a CoE could facilitate would broaden the scope of possibilities for all Allies and allow otherwise unaffordable development or customisation of AI-technologies.

How could the CoE be organised?

The *Centre* would essentially guide the transatlantic community through the path of political, economic and technological challenges as it (ideally) seeks to integrate multinational and multidisciplinary (industrial, military and governmental) expertise to understand AI in its full complexity. **The Centre of Excellence would provide the foundation of expertise** for future strategic risk assessment, policy planning and capability review process for all its primary stakeholders. These are NATO and EU member states, likeminded associated state actors, industrial leaders and specialised international organisations (EDA, NATO ACT and others).

The organisational structure of the *Centre of Excellence for AI* would most likely be based on the structures of existing NATO and EU policy advisory bodies – in most cases also labelled as Centres of Excellence – with the *NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE)* being the most similar candidate.

This is due to the **relative proximity (and interrelation) between cyber and AI in the terms of their common existential (digital) domain**. In keeping with previous CoEs, a coalition of willing (and likeminded) transatlantic allies should be led by one member that oversees the formal aspects of efforts to establish and host the *Centre*. Other stakeholders could join the *Centre* and capitalise on its expertise while also contributing to its efforts and overall mission.

From the outset, the *Centre* requires a solid and objective political understanding of the coming impact and unavoidability of transformative technology on the nature of (in)security. Building such an understanding is, as we believe, one of the key tasks of the transatlantic defence and security policy community interested in providing our leaders with insightful and objective assessment of future challenges. AI will arguably not replace the challenges of our past, but it clearly has the decisive potential to increase the complexity of those we will be striving to address in the future. And that future might not be very distant one. Hence, the call for a *Centre of Excellence for AI* is as strong as it is imminent.

James Townsend is former US Deputy Assistant Secretary of Defense for European and NATO Policy and currently an Adjunct Senior Fellow at Center for New American Security.

Alena Kudzko is Deputy Research Director at the GLOBSEC Policy Institute

Tomáš A. Nagy is Research Fellow for Defence and Security at the GLOBSEC Policy Institute