ACTIVITY REPORT

NAADSN
North American and Arctic Defence and Security Network

naadsn.ca

October 8, 2024

NATO at 75: Adapting to the Future of Technology

Benjamin Johnson, Ph.D.
NAADSN Fellow

On Tuesday, October 1, 2024, the Henry M. Jackson School of International Studies at the University of Washington hosted a delegation of NATO officials and other guests to discuss current challenges.[i] This piece reflects on that symposium and its discussions, focusing on NATO's force modernization and the role of technology, specifically artificial intelligence (AI) and quantum technology (QT).

Background

NATO was founded in 1949 in the aftermath of two world wars through the newly emerged bipolar world order with nuclear weapons proliferation on the horizon. NATO's core purpose of providing a collective defence to its members dovetailed with its commitment to democratization, freedom, and a rules-based international order as the foundation for peace. However, the end of the Cold War led to speculation on the alliance's future, given that its key adversary had dissolved in the momentum of Fukuyama's prophesized (but premature) *end of history*.[ii]

New events and trends during the 1990s and early 2000s quickly shifted NATO's focus and forced it to adapt to the emerging security environment.[iii] Now, seventy-five years after its founding, NATO once again finds itself in a similar position, forced to adapt to a quickly changing world.

Throughout the symposium, the war in Ukraine (unsurprisingly) dominated many discussions, as did China's rise. Indeed, while recognizing NATO's recent shift to acknowledge and address China, it was remarked that China is "*the* security threat of the 21st century." Indeed, China's rapid rise as a major state power and Russia's full-scale invasion of Ukraine firmly reassert the role of major power competition in shaping the contemporary security environment.

This environment is further complicated by other geopolitical actors and events (such as the BRICS and ongoing violence in Africa and the Middle East) while trends related to technology, social cohesion, economic (dis)integration, climate change, and others merge in messy and difficult-to-anticipate ways to stoke local,

regional, and international tensions. Thus, NATO is at a crossroads. How it adapts to and meets the challenges of this complex and unstable security environment will shape the next seventy-five years of the alliance and the security of its partners.

Adapting to the Future

Given the increasing connection and speed of globalization, NATO is adapting and planning capabilities for operating in multiple places across all domains simultaneously, in line with its 360-degree approach adopted during the 2022 Madrid Summit.[iv] Threats are no longer confined to single scales or geographies as everything is interconnected. Consequently, NATO is increasingly concerned with operational theatres beyond its traditional policy scope, such as the Arctic[v] and Indo-Pacific.

NATO must maintain its force advantage to deter aggression and defend itself successfully. The key dimensions of this advantage are speed and scale, meaning that NATO forces must be able to adapt and respond with increasing velocity over greater distances, reflecting the multifaceted and networked character of the threat environment.[vi]

Underpinning these themes is the place of technology and its role in force modernization. Technology is both a threat and an opportunity. Much of the NATO symposium discussion prioritized NATO's relationship with industry to produce the innovation necessary for maintaining and enhancing its force advantage while achieving 360-degree awareness, especially using AI and potentially QT in the future.

Several speakers commented on well-known problems related to procurement delays, scaling and commercialization development, the speed of technical upgrades, adopting new technologies, and cultural asymmetries between public institutions and the private sector. Solutions for alleviating these issues focused on building and expanding industry and academic relationships with NATO and other military research labs. Discussants also focused on enabling industry the freedom and flexibility to be innovative and learn from field testing technologies in an iterative fashion, including through battlefield deployment.

Challenges

Within the symposium, challenges to NATO's future were largely framed as technical and institutional in nature. Industry, for its part, is historically opposed to regulation based on the idea that markets allow for the flexibility of creative destruction, whereas institutions are designed for stability over long time periods but sacrifice agility and the ability to adapt to new circumstances rapidly. From a techno-institutionalist angle, industry requires distance from regulatory and bureaucratic limits to innovate at speed and scale. As large and complex organizations, bureaucracies and the public sector typically suffer from institutional lag or inertia as they may resist developing or implementing new technologies while bureaucratic siloing and cultural asymmetries create added inefficiencies. From some perspectives, in an ideal-type relationship, industry leads innovation and scaling while the public sector funds and provides many resources for a technology’s development until it can be successfully commercialized.

While important, there are notable limits to framing NATO's challenges in strictly technical and institutional terms.

There is a tendency (historically and currently) to treat technology as a panacea for all problems. Many technological revolutions go underrealized, and those that happen are often unexpected. While there is broad recognition that it is difficult to anticipate and accurately plan for the technological disruptions potentially brought by AI and quantum, it must be reiterated that they may not fulfill the lofty promises of or function according to their hype. This issue is particularly relevant for military adoption of AI and its role in multi-domain awareness and decision-making.

There has been a conspicuous lack of commentary or discussion on the values and ethics with which NATO and allied states should develop and use AI and quantum technologies. NATO has developed its principles of responsible AI, focusing on bias mitigation, transparency, and accountability.[vii] Nonetheless, several practical and theoretical problems remain as those parameters are ill-defined and involve significant contextual differences depending on where and how AI systems are deployed.

Whether and where humans should be "in" or "on the loop" of military systems (including, but not limited to autonomous weapons systems) is as much a political and ethical question as it is a technical one that still lacks a satisfactory resolution. Even framing that issue as whether and where to place humans in AI systems may be inappropriate. The complete separation between humans and machines as discrete entities in a decision-action chain is impossible, given that algorithms, their underlying data, and development are thoroughly mediated and laboured upon by humans.

Values and ethics are also socially and institutionally bounded, including within NATO's mandate to support democracy, freedom, and other universal rights. These values define NATO and its members relative to other actors (particularly among autocratic regimes) seeking to normalize and mobilize antithetical belief systems for their benefit.

Framing NATO's challenges as inherently technical and institutional through organizational functions and culture can create potential contradictions, opening more space for private industry to shape the normative and value-based conditions of technological development and use. While industry is an important partner, it should not be assumed that its interests necessarily merge with public or security interests, particularly given its alignment to the profit motive versus wider considerations and the complex reality of its multinational linkages. Ongoing disagreements between governments and big data actors like Meta and Google are evidence of this issue.

Opportunities

While NATO and its allies have primarily focused on leading in technological innovation in the AI and quantum sectors, they also have the potential to be influential norm shapers rather than passive adapters. While NATO's principles of responsible AI development are a welcome start to this endeavour, more is needed, particularly as bias and responsibility are ill-defined concepts in the AI policy landscape, especially in the military sphere.

Further, universalizing these values will prove challenging as AI and quantum are not singular technologies but entire ecosystems, and the principles of their development and use will shift depending on their function and situation. These fundamentally political and ethical questions take on unique meanings depending on context. AI, quantum, and other technologies are not neutral materials or tools but are driven, operated, and filtered through social relations and institutions.

NATO is shaped as much by its values as it is by material notions of power, advantage, and defence. It will be essential to ensure those values align with the development and operation of AI, quantum, and other new technologies as they emerge and scale across different sectors. Speed and competition are powerful incentives for advancing technological innovation, but they also act as a seductive logic that risks prioritizing that innovation above all other considerations. As NATO thinks about its next 75 years, it must be mindful not to narrowly subscribe all of its thinking and policymaking on force modernization to that seductive logic if it is to accurately reflect those values it holds so dear.

---

[i] The symposium was titled NATO and the Future of American Security. Speakers included Gen. Chris Badia, *Deputy Supreme Allied Commander Transformation*, NATO Allied Command Transformation; Dr. Vlasta Zkulic, *Head of Strategic Issues and Engagements*, NATO Allied Command Transformation; and a keynote address from The Hon. Adam Smith, *Ranking Member, House Armed Services Committee*, United States House of Representatives.

[ii] Francis Fukuyama. (2006). *The End of History and the Last Man*. Free Press: New York, London, Toronto, Sydney.

[iii] The Yugoslav wars, the Rwandan genocide and the development of the responsibility to protect (R2P) as a guiding framework of human security, the September 11, 2001, terrorist attacks, the war in Afghanistan, and environmental degradation, among other trends and events, shifted NATO beyond collective deterrence into a much-broadened security agenda.

[iv] NATO 2022 Strategic Concept. Available at https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

[v] For a recent discussion on NATO's role in the Arctic, see Gabriella Gricius. June 7, 2024. NATO in the Arctic. NAADSN Policy Primer. https://www.naadsn.ca/wp-content/uploads/2024/10/24_Jun_Gricius_Policy-Primer-NATO-Arctic.pdf

[vi] The increasing interconnections of the security environment have long been noted and linked to changes in strategic doctrines focused on adaptation and resilience through 'network' warfare.

[vii] See Summary of NATO's revised Artificial Intelligence (AI) strategy. July 10, 2024. https://www.nato.int/cps/en/natohq/official_texts_227237.htm