doi:10.1017/aju.2020.27

SYMPOSIUM: HOW WILL ARTIFICIAL INTELLIGENCE AFFECT INTERNATIONAL LAW?

AI'S IMPACT ON MULTILATERAL MILITARY COOPERATION: EXPERIENCE FROM NATO

*Steven Hill**

AI-based military applications present both opportunities and challenges for multinational military cooperation. This contribution takes stock of the state of discussions around AI-based military applications within the North Atlantic Treaty Organization (NATO). While there have been a number of recent developments in national AI strategies and policies, discussions at the NATO level are still in early phases, and there is no agreed NATO policy in this area. Further multilateral work is needed if like-minded states such as NATO Allies and partners are to head off the serious risk that disagreements about these technologies might hamper effective multilateral military cooperation.

This essay first frames the overall strategic context within which discussions related to AI at NATO take place. Perceptions of security threats are shifting as a result of the rise of great power competition. At the same time, the AI policies of some individual Allies are rapidly evolving. The essay then describes the publicly-accessible work that has taken place within NATO on AI issues. It uses two potential military applications of AI that are likely to be of interest in a NATO context, as well as some positive and negative elements associated with them. Finally, the essay suggests the need for continued multilateral dialogue on military use of AI.

The Strategic Context at NATO

NATO is an alliance of thirty states that has collective defense as one of its three core tasks.[1] Part of NATO's identity is as "an alliance that constantly modernises and adapts to new threats and challenges,"[2] including those arising from the development of new technologies. As Allied Heads of State and Government put it at their meeting in December 2019 in London, "To stay secure, we must look to the future together. We are addressing the breadth and scale of new technologies to maintain our technological edge, while preserving our values and norms."[3]

These two short sentences contain at least four different ideas that shed light on NATO's strategic approach to AI. First, they emphasize maintaining "our" technical edge. This could be interpreted as referring to the collective

* *The author served until February 2020 as Legal Adviser and Director of the Office of Legal Affairs (OLA) at the NATO International Staff in Brussels.* *This essay is based on work done with Nadia Marsan of OLA, whose contributions the author gratefully acknowledges. See, e.g., Nadia Marsan & Steven Hill, International Law and Military Applications of Artificial Intelligence, in* THE BRAIN AND THE PROCESSOR: UNPACKING THE CHALLENGES OF HUMAN-MACHINE INTERACTION *(Andrea Gilli ed., 2019). The author also thanks Mark Norris of OLA and Ally Berman of Emory University for research assistance. This essay represents the author's personal views and does not necessarily reflect the views of NATO or its Allies.*

[1] *See, e.g.*, NATO, STRATEGIC CONCEPT (Nov. 19, 2010) (setting forth the Alliance's three core tasks).

[2] NATO, Brussels Summit Declaration, para. 79 (July 11, 2018).

[3] NATO, London Declaration, para. 6 (Dec. 4, 2019).

© Steven Hill 2020. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

https://doi.org/10.1017/aju.2020.27 Published online by Cambridge University Press

advantage that NATO Allies enjoy or to the advantage that individual member states have. Second, the emphasis on maintaining an edge hints at the growing importance of great-power competition in NATO's strategic thinking, especially with regard to China. The Alliance increasingly has turned its attention to China, with NATO leaders adopting historic language at the London Summit about the "opportunities and challenges" posed by China.[4] Technological competition, including in the AI field, where China has made major advances, is one of these areas. Third, the statement refers to the need to "preserv[e] our values and norms" while dealing with the new technology. While not going into detail about what those values and norms are, this language flags the importance of legal and ethical considerations in working together. Finally, the statement has an express reference to the need for multilateral cooperation in this space going forward: "we must look to the future together."

Another element of the strategic context is the rapid proliferation of national military AI strategies adopted by individual NATO Allies. Many of these strategies explicitly include legal and ethical components. For example, France's recent strategy on AI and defense sets forth three major principles: (1) respect for international law; (2) the presence sufficient human control; and (3) ensuring responsibility of human command. France is also working to create a defense-focused ministerial ethics committee whose purpose will be to discuss the implications of emerging technologies in the defense field.[5] The 2018 German AI strategy—which is general in scope, not specific to the defense sector—refers to the need to "integrat[e] AI in society in ethical, legal, cultural and institutional terms in the context of a broad societal dialogue and active political measures."[6] In the United States, the Department of Defense recently adopted five principles that the Defense Innovation Board proposed to govern the development of AI systems in defense, emphasizing that such development must be: (1) responsible; (2) equitable; (3) traceable; (4) reliable; and (5) governable.[7] While these strategies use some of the same categories of terms and thus appear to speak the same language, it is not clear to what extent states would agree about how to apply such principles in the context of a specific military use of AI.

While these strategies are developed to govern work at the national level, they also tend to refer—if only in general terms—to the need for multilateral cooperation. The U.S. Department of Defense's Joint Artificial Intelligence Center, for example, articulated as one of the pillars of its strategic approach "evolving our crucial international alliances and partnerships abroad. An extended network of mutually beneficial alliances and partnerships provides a durable means of overcoming global AI challenges, deterring aggression, and supporting stability through cooperation."[8] While the European Commission's February 2020 AI White Paper excludes military AI from its scope,[9] a food-for-thought paper on AI developed during the 2019 Finnish presidency of the European Union emphasizes the importance of cooperation with partners, including as part of the increasing trend toward EU-NATO cooperation.[10]

[4] *Id.* at para. 6 ("We recognise that China's growing influence and international policies present both opportunities and challenges that we need to address together as an Alliance.").

[5] *See* The Ministry of Armed Forces Presents its New Strategy for Artificial Intelligence, Permanent Representation of France to NATO (Apr. 5, 2019).

[6] The Federal Government's Artificial Intelligence Strategy: AI Made in Germany, German Federal Ministry for Economic Affairs and Energy (Dec. 4, 2018).

[7] *See* C. Todd Lopez, *DOD Adopts 5 Principles of Artificial Intelligence Ethics*, DOD News (Feb. 25, 2020).

[8] U.S. Department of Defense, Summary of the 2018 Department of Defense Artificial Intelligence Strategy (Feb. 12, 2019).

[9] Eur. Comm'n, *White Paper on Artificial Intelligence – A European Approach to Excellence and Trust*, COM (2020) 65 final (Feb. 19, 2020).

[10] Finland, Estonia, France, Germany & The Netherlands, Digitalization and Artificial Intelligence in Defence (May 17, 2019). On potential areas of NATO-EU cooperation, *see* Eur. Union Inst. for Security Studies, *The EU, NATO and Artificial Intelligence: New Possibilities for Cooperation?* (Nov. 14, 2019).

https://doi.org/10.1017/aju.2020.27 Published online by Cambridge University Press

NATO Activities to Date

If NATO Allies must look to the future of new technologies together and if national strategies are calling for more international cooperation, it is worth asking what they have done together to date. Allied Command Transformation (ACT), one of NATO's two strategic commands,[11] has played a leading role in NATO's work on innovation and disruptive technologies, including AI. In October 2019, for example, ACT organized an informal workshop with NATO ambassadors and military representatives.[12] The focus of the event was "the Alliance's efforts to leverage the power of data science, machine learning and other new technologies to improve its decision-making."[13] This event followed up on a similar informal workshop held in March 2018 designed to highlight the broader impact of the development of disruptive technologies on the Alliance.[14] One take-away from this informal discussion was that allies may wish to discuss some of the legal implications of this emerging technology in a multilateral forum such as NATO.

On the level of policy documents, NATO has developed an "Emerging and Disruptive Technologies Roadmap" that is meant to guide future Alliance work in this area. As ACT describes it, the Roadmap "uses a bottom-up approach to conduct rapid and tangible demonstrations in realistic operational conditions in order to understand the potential of Emerging and Disruptive Technologies from both the opportunity and threat standpoints and to set the conditions to use them within NATO and its Member Nations."[15] This could include drawing out some commonly accepted legal and ethical principles surrounding the military use of AI such as respect for international law, the need to keep humans in the loop, and the importance of clear accountability. More broadly, NATO is actively working to develop a data policy, specifically to put in place standards relating to the oversight of multinational pooling and sharing of data.[16]

Finally, in terms of training and exercises, NATO is also now regularly integrating new technology in its exercises, especially in the area of humanitarian assistance. For example, a NATO disaster response exercise held in Serbia in October 2018 successfully incorporated disaster relief tools powered by artificial intelligence such as the processing of aerial images of the simulated disaster site in order to identify victims more quickly.[17]

AI Applications from a NATO Perspective

It is useful to complement this description of NATO's fairly nascent policy work on military applications of AI with a brief overview of the types of applications that one hears most discussed in NATO circles. Given the amount of academic, media, and political attention to the issue of lethal autonomous weapons systems (LAWS), it might come as a surprise that it is the far less high-profile or headline-grabbing applications of AI that receive attention within NATO. This may well be because LAWS are already being discussed by a Group of Governmental Experts within the Geneva-based framework of the Convention on Certain Conventional

[11] ACT is based in Norfolk, Virginia. NATO's other strategic command is Allied Command Operations located at the Supreme Headquarters Allied Powers Europe in Belgium.

[12] NATO, NATO Ambassadors and Military Leaders Meet to Discuss Disruptive Technologies (Oct. 2, 2019).

[13] *Id.*

[14] *See* NATO, SACT's Opening Remarks to the NAC/MC Away Day (Mar. 22, 2018).

[15] ACT, NATO Defense Ministers' Meeting (June 27, 2019).

[16] *See, e.g.*, Joel Gehrke, *NATO Official Calls for "Massive Collection of Data" in Order to Maintain Military Edge*, WASH. EXAMINER (Feb. 20, 2020).

[17] *See* NATO, Remarks by NATO Deputy Secretary General Rose Gottemoeller at the Xiangshan Forum in Beijing, China (Oct. 25, 2018).

https://doi.org/10.1017/aju.2020.27 Published online by Cambridge University Press

Weapons, thus making Allies hesitant to duplicate discussions in Brussels. However, the reason that the issue of LAWS—however important the debates involved—is not on the forefront of the agenda at NATO is likely more straightforward: that current and foreseeable technology suggests different, perhaps more prosaic applications, for AI in the military sphere. This essay focuses on two: (1) intelligence, surveillance, and reconnaissance (ISR); and (2) cyber defense. The development and use of AI-enabled applications in each of these areas clearly presents both opportunities and challenges.

Enhancing the information available to support decision-making is one of NATO's priorities. ISR is based on information-gathering from a variety of assets deployed across domains. The information or data gathered from both NATO and national assets can then be fused together to help identify patterns and trends in support of situational awareness and operational decision-making. Since this data will likely be too voluminous for traditional human analysis, NATO can leverage AI-enabled systems to comb through these datasets. In this way, NATO can apply AI to enhance situational awareness and improve decision-making, a potentially considerable advantage given the challenges of getting all Allies up to speed on rapidly evolving situations.

AI applications can also be used in the context of cyber defense, where NATO has a defensive mandate focused on defending NATO's networks and supporting Allies as they defend their own networks. AI-based applications cover areas such as preemptive patching and the taking of corrective action on the basis of a constant analysis of low-level and recurrent patterns of attacks and cyber threats across networks, all done more quickly and with greater precision. Moreover, the more information exchanged on the nature of attacks in a variety of networks, the easier it is to identify trends in multinational cyber threats.

While the use of AI in both these contexts could potentially increase the speed and quality of multinational military cooperation, it clearly also can pose difficulties. For example, increasing speed could be perceived as fueling pressure for inappropriately accelerated action. This kind of acceleration of usual processes might be perceived as going against "normal" NATO decision-making in a number of ways: it might be seen as evading the political control exercised by the North Atlantic Council, overriding the consensus decision-making that applied within the Alliance, being susceptible to misinterpretation or being seen as escalatory in nature, or otherwise leading to unpredictable results. In an extreme case, Allies might see these situations as inconsistent with NATO's collective defense mandate. This might result in a backlash against the use of AI-enabled military applications, precisely at a time when the Alliance needs to maintain an edge with them. In other words, as with many issues involved in multinational military cooperation, the problem may ultimately boil down to one of trust.

Conclusion: The Need for Multinational Dialogue

As noted above, the different national strategies refer to the need for legal and ethical frameworks. They also generally refer to the desirability of multilateral cooperation on AI. The limited work within NATO so far has also pointed to a willingness to take on these issues in a multinational setting. However, the reality is that these discussions have not yet taken off. There may be good reasons for this, including the ongoing nature of LAWS discussions in Geneva or the understandable reluctance—frequently encountered with respect to new technologies—to take positions that could constrain innovation or that could present a strategic disadvantage to those who abide by the rules.

At the same time, the perception that there are unresolved legal or ethical issues hovering over military applications of AI clearly poses a risk to the use of this technology, including in a multilateral military setting. There is generally broad agreement among NATO allies that existing international law should apply to the military use of new technologies, including AI. However, a perception of lack of clarity on the rules of the game may lead to a lack of trust that might hamper multinational cooperation. In this regard, dialogue about legal and ethical frameworks can be an important means of building trust.

https://doi.org/10.1017/aju.2020.27 Published online by Cambridge University Press

Individual NATO Allies are in the midst of developing their own national strategies for military applications of AI. As noted above, while these strategies use some of the same vocabulary in calling for more clarity on the legal and ethical frameworks of military AI, there is a real risk of a lack of meeting of the minds about the substantive content of these frameworks.

Consider but one of the issues that will arise: the potential scope of difference of views related to data ownership, sharing, and use.[18] If data is "fuel" for AI, the question of who owns it and under what conditions it can be shared and used by others is of strategic importance. Despite the sense that like-minded countries will need to cooperate to develop their own sources of such "fuel," there is no agreed transatlantic approach in policy and law on how to handle a wide range of data-related legal issues. Data sharing arrangements need to be in place beyond the limited, generally law enforcement-related sectors in which there are existing arrangements. There is considerable work to be done to create the necessary trust to develop mutually-agreed procedures that strike the balance between the many different equities involved in such an exchange of information.

While most of these discussions on data take place outside of NATO, NATO does have some experience that could be relevant. For example, NATO already has in place mechanisms for the secure sharing of information that are based on trust built over the life of a seventy-year-old Alliance. NATO has recently built upon these practices to promote the sharing of evidence gathered in battlefield settings for use in the criminal prosecutions of foreign terrorist fighters.[19] Achieving consensus agreement on these initiatives required a considerable amount of legal dialogue for Allies to find a pragmatic way forward, building on NATO's tradition of "legal interoperability."[20]

In the end, NATO's early-days experience shows that in a multinational setting, it is important to understand AI-enabled military applications and to support their implementation in practical contexts. This requires open dialogue between Allies and other partners as well as with industry. NATO has the potential to play a unique role in this process.

[18] *See* Steven Hill, *Transatlantic Interoperability Challenges in the Law of Armed Conflict in 2040* (Lieber Institute, forthcoming 2020) (citing transatlantic differences over data as one of three strategic trends that will affect the future of law of armed conflict).

[19] *See, e.g.*, Juliette Bird, *Working with Partners to Counter Terrorism*, NATO Rev. (May 16, 2019).

[20] *See, e.g.*, Peter Olson, *Convergence and Conflicts of Human Rights and International Humanitarian Law in Military Operations: A NATO Perspective*, *in* Convergence and Conflicts of Human Rights and International Humanitarian Law in Military Operations 254 (Erica de Wet & Jan Kleffner eds., 2014) (noting that "NATO addresses legal questions . . . pragmatically rather than doctrinally . . . . [R]ather than requiring adherence to a single common body of law, the Alliance's expectation is that all States participating in a NATO or NATO-led operation will act lawfully within the legal framework applicable to them").

https://doi.org/10.1017/aju.2020.27 Published online by Cambridge University Press