Artificial Intelligence and Accountability: A Multinational Legal Perspective

Mr. Steven Hill / Mrs. Nadia Marsan[1]
Office of Legal Affairs
NATO Headquarters
Boulevard Léopold III, 1110, 1130 Evere
BELGIUM

e-mail: hill.steven@hq.nato.int / marsan.nadia@hq.nato.int

ABSTRACT

*This paper supports the specialist meeting on **Big Data and Artificial Intelligence for Military Decision Making** by exploring the legal implications of new technology on NATO decision making. The paper begins by presenting the concept of "legal interoperability," one of the tools that legal advisers working in NATO seek to promote. It then introduces some of the current legal issues and debates surrounding the development and use of AI, including the difficulty in defining key concepts arising out of the increased use of AI such as "autonomy," and questions pertaining to accountability. Finally, this paper examines how further dialogue among Allies and with NATO partners can contribute to the development of a reliable approach on accountability issues related to AI-enabled technology. The paper argues that given the rapidly evolving technology and the asymmetric approach and capabilities of nations, efforts within the Alliance should focus on ensuring NATO's "legal preparedness" so that collective action is not thwarted by legal hurdles and mismatched legal approaches amongst Allies.*

INTRODUCTION

In the 2016 Warsaw Summit Communiqué, NATO Heads of State and Government recognized that "the changed and evolving security environment demands the ability to meet challenges and threats of any kind and from any direction".[2] As an Alliance of 29 Nations focused on collective defense as one of its core tasks, NATO must be prepared to address emerging threats and security challenges arising from the development of new technologies. Among these, the development and use of Artificial Intelligence (AI) presents both opportunities and challenges to the North Atlantic security landscape. On 22 March 2018, Allied Command Transformation, NATO's adaptation hub located in Norfolk, Virginia in the United States of America, organized an informal workshop with NATO Ambassadors and Military Representatives to discuss the impact of the development of disruptive technologies on the Alliance. One question raised concerned the interoperability challenges NATO could face as Allies develop disruptive technology with differing capabilities. A take-away from the discussion is that Nations may wish to discuss some of the legal implications of this emerging technology in a multilaterally forum such as NATO.

We have already witnessed the effect that the development and use of AI is having on Allied security: the recent revelations regarding the use of Facebook data by a consulting firm for political leverage show that

[1] Steven Hill is the Legal Adviser and Director, Office of Legal Affairs, North Atlantic Treaty Organization, NATO Headquarters, Brussels. Nadia Marsan is Senior Assistant Legal Adviser in the NATO Office of Legal Affairs. The views expressed in this article are ours alone and do not necessarily represent the views of NATO or its Allies. We gratefully acknowledge the support provided by Elif Ece Ozturk of the NATO Office of Legal Affairs.

[2] Warsaw Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8-9 July 2016, Press Release (2016)100, at para 6. Available at: www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en.

automated data processes providing sophisticated profiling of individuals can be used to manipulate the fundamental elements of democracy, with potentially profound effects on security. How Allies respond to this changed security environment, both individually and collectively, raises a number of legal questions. The cross-cutting nature and widespread impact of AI-enabled technologies necessitates multinational discussion and debate. For now, these debates are fueled by the absence of State practice and jurisprudence on the development and use of AI-enabled technology. Multinational organizations such as NATO can provide a venue for discussion amongst Allies, providing a forum where States can express their views on these issues from a military and security perspective. As of yet, there are no NATO policies providing guidance on how to address the development and use of AI technology. Consequently, this paper provides some preliminary observations from the personal perspective of NATO legal advisers who have begun to encounter these issues rather than on the basis of agreed NATO positions or doctrine. It is therefore intended to introduce rather than resolve some of the key legal issues that are likely to arise in future AI-related discussions within NATO.

This paper begins by presenting the concept of "legal interoperability," one of the tools that legal advisers working in NATO seek to promote. It then introduces some of the current legal issues and debates surrounding the development and use of AI, including the difficulty in defining key concepts arising out of the increased use of AI such as "autonomy," and questions pertaining to accountability.[3] Finally, this paper examines how further dialogue among Allies and with NATO partners can contribute to the development of a reliable approach on accountability issues related to AI-enabled technology. The paper argues that given the rapidly evolving technology and the asymmetric approach and capabilities of nations on the matter, efforts within the Alliance should focus on ensuring NATO's "legal preparedness" so that collective action is not thwarted by legal hurdles and mismatched legal approaches.

1.0 THE NATO CONTEXT: LEGAL INTEROPERABILITY

NATO is an Alliance of values, and one of the core values that the Alliance defends is the rule of law. The commitment to respect the rule of law is enshrined in the preamble to the 1949 North Atlantic Treaty and is reaffirmed in declarations by NATO Heads of State and Government at their regular Summit meetings. It is a key element of NATO and NATO-led operations and is necessary to ensuring legitimacy and securing public support. Compliance with international law is an essential component of NATO's success in all of its endeavours and activities. Correspondingly, the demand for legal advice from over 70 legal offices that make up the NATO legal community has never been higher. The scope of issues on which the typical NATO legal adviser is called to advise on can be daunting and guidance on Allied views is not always available, especially in an easy-to-access consolidated format. This is especially true in the context of emerging technologies such as the security impact of AI-enabled tools. Under the auspices of the NATO Office of Legal Affairs, NATO has launched and reinvigorated a number of legal dialogues, including with Allies, partner nations and international organisations. Such legal dialogues are essential to understanding Allies' potentially conflicting legal postures.

NATO Allies each have their sovereign domestic legal systems and are bound by different international legal obligations. Allies also often have their own understanding on what international law obligations are applicable to them and under what conditions. As an alliance of 29 nations, NATO takes all decisions by consensus and the main challenge in such a multilateral environment is enabling Nations to act together in line with the individual legal obligations of each, taking account of the differences in applicable legal

[3] Much has been written on this, with respect to autonomous weapons systems (AWS). There is much ongoing work in this area, namely in the context of the United Nations Group of Government Experts on Lethal Autonomous Weapons Systems. NATO Allies are directly participating in these discussions and until national positions on the development and use of LAWS have solidified, Allies will be reluctant to bring such questions for resolution within a multilateral organization such as NATO. Therefore, for the purposes of this paper, the discussion will focus rather on the broader discussion of the legal issues pertaining to the military development and use of AI-enabled technologies.

parameters. A key technique that legal advisers use to help achieve consensus despite these legal differences is "legal interoperability".

"Legal interoperability" is derived from the military concept of interoperability of forces, whereby the military forces of the 29 Allies are able to work together to achieve common objectives. NATO doctrine defines the interoperability of forces as "[t]he ability of the forces of two or more nations to train, exercise and operate effectively together in the execution of assigned missions and tasks."[4] In the Warsaw Summit Communiqué, Allied Heads of State and Government referred to the need for interoperability to accomplish NATO's goals. Within NATO, there is often a diversity of legal views on core issues of international law. Let us take, for example, the laws of war, where 27 of NATO's 29 Allies are party to the Additional Protocols to the Geneva Conventions. This challenge is also reflected in International Criminal Law as the Rome Statute establishing the International Criminal Court is likewise adopted only by 27 Allies. As a military Alliance founded on the rule of law, these sometimes different legal obligations can be challenging. The challenges are especially daunting when there is a need for a rapid decision by Allies based on collective consensus and requiring legal justification.

NATO' *raison d'être* is collective defence, and legal interoperability is one of the key enablers for the Alliance. From a legal perspective, interoperability refers to the need for Nations to work together in a variety of contexts despite the application of differing legal frameworks and obligations. As one observer of NATO operational law defined it, "'[l]egal interoperability' is understood … as the ability of the forces of two or more nations to operate effectively together in the execution of assigned missions and tasks and with full respect for their legal obligations, notwithstanding the fact that nations concerned have varying legal obligations and varying interpretations of these obligations." [5] Legal interoperability relies on a broad understanding of those areas of legal divergence amongst Allies, which requires careful analysis of the legal positions expressed by the relevant Nations. In the case of new technologies, this understanding is difficult to acquire, in part because Nations have not had the opportunity to set forth their legal views or have refrained from doing so in order to prevent the loss of a potential technological edge. Within NATO, legal interoperability has proven to be indispensable to rapid decision-making and is facilitated by Allies' pragmatism when faced with questions of collective security, emphasizing and relying on those elements that are common to all rather than on those elements of divergence.

2.0 DEFINITIONS

The first issue that arises in the context of AI which highlights the difficulty in setting a clear conceptual scope and applicable legal parameters, is a definitional one. There are no internationally agreed legal definitions for the core concept of AI. The lack of agreed legal definitions can hinder and stall discussions in part because Nations may rightfully be hesitant to commit to the regulation of a new technology when the scope and the evolution of that technology is not clear.

While there might not be agreed legal definitions of AI, broader discussions on AI have identified a number of elements that can nevertheless provide some preliminary guidance. The first suggested definition of AI is, "the capability of a computer system to perform tasks that normally require human intelligence, such as visual perception, speech recognition and decision-making."[6] The second definition of AI which is useful here is, "technologies that enable machine learning, natural language processing, deduction through vast

[4] NATO Standardisation Office, NATO Glossary of Terms and Definitions, AAP-06(2014).

[5] M. Zwanenburg, "International humanitarian law interoperability in multinational operations", *International Review of the Red Cross*, 95 (2013), 681-4.

[6] M. L. Cummings, *Artificial Intelligence and the Future of Warfare*, International Security Department and US and the Americas Programme, January 2017, at page 3. Available at https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf

data-computational power, and ultimately, automated decision-making in robotics or software that can substitute for tasks once performed exclusively by human action and judgement".[7]

Another term that is important to define is "autonomy". The concept of autonomy is key to AI because it is precisely the technological edge provided by AI that enables autonomy or, expressed another way, enables the independent action of a machine. Autonomy itself can be defined as "the ability of a system, platform or software to complete a task without human intervention, using behaviours resulting from the interaction of computer programming with the external environment".[8] Although beyond the scope of this paper, other definitions incorporate key concepts in the military use and development of AI.[9]

These preliminary definitions suggest that AI is about replicating human perception, cognition and decision-making as well as introducing a certain element of independence to these systems. Although the modelling of human intelligence provides opportunities from a security perspective, these are also fraught with challenges that are only beginning to be understood: "there is now a broad consensus that AI research is progressing steadily, and that its impact on society is likely to increase. The potential benefits are huge, since everything that civilization has to offer is a product of human intelligence; we cannot predict what we might achieve when this intelligence is magnified by the tools AI may provide, but the eradication of disease and poverty are not unfathomable. Because of the great potential of AI, it is important to research how to reap its benefits while avoiding potential pitfalls". [10]

3.0 LEGAL IMPLICATIONS ARISING FROM SPECIFIC USES OF AI

There are already applications of AI that are of interest to a multilateral security organisation such as NATO. Acknowledging the absence of a clear consensus on the legal definition of AI, it is useful to highlight some concrete areas where AI has been and is currently being used with effects, both positive and negative, on Allied security.[11] Three areas of AI-enabled technologies are worth mentioning here: intelligence, surveillance and reconnaissance; the manipulation of personal data; and, disinformation.

Intelligence, Surveillance and Reconnaissance (ISR)

[7] B. Scott, S. Heumann and P. Lorenz, *Artificial Intelligence and Foreign Policy*, Stiftung Neue Verantwortung, January 2018. Available at: https://www.stiftung-nv.de/sites/default/files/ai_foreign_policy.pdf

[8] Multinational Capability Development Campaign (2013-2014), "Role of Autonomous Systems in Gaining Operational Access, Policy Guidance (MCDC Policy Guidance): Autonomy in Defense Systems", 29 October 2014, p. 9, available at: https://innovationhub-act.org/sites/default/files/u4/Policy%20Guidance%20-%20Autonomy%20in%20Defence%20Systems%20MCDC%202013-2014.pdf

[9] For example, the definition of autonomous weapons systems is also further qualified by the introduction of the "lethal" elements. The United States Department of Defense Directive defines lethal autonomous weapons systems (LAWS) as, "weapon system that, once activated, can select and engage targets without further intervention by a human operator." See DoD Directive 3000.09, "Autonomy in Weapon Systems", November 21, 2012. The International Committee of the Red Cross (ICRC) has defined AWS as "any weapon system with autonomy in its critical functions—that is, a weapon system that can select (i.e. search for or detect, identify, track, select) and attack (i.e. use force against, neutralize, damage or destroy) targets without human intervention." See ICRC, "Views of the International Committee of the Red Cross (ICRC) on autonomous weapon system", 11 April 2016 at page 1. Available at: https://www.icrc.org/en/document/views-icrc-autonomous-weapon-system.

[10] See S. Russel, D. Dewey and M. Tegmark, Research Priorities for Robust and Beneficial Artificial Intelligence, Association for the Advancement of Artificial Intelligence, Winter 2015 at page 106. Available at: https://futureoflife.org/data/documents/research_priorities.pdf?x92422. This text was incorporated in the Open Letter on the Research Priorities for Robust and Beneficial Artificial Intelligence, available at: https://futureoflife.org/ai-open-letter/.

[11] The following examples are drawn from: G. Allen and T. Chan, *Artificial Intelligence and National Security*, Harvard Kennedy School, Belfer Center Study, July 2017, available at: https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf.

Effective security and military decision making depends on reliable situational awareness. In recent years, technological developments have enabled the autonomous collection of massive amounts of data, including measurements, satellite and infrared imagery, and electronic signals, through ISR systems, such as unmanned aerial vehicles (UAV) and satellites. The ISR process begins with information gathering through sensors to intelligence analysis where the information is brought together towards supporting effective operational decision-making. The increased autonomy of sensors calls for an equivalent autonomy in analysis through systems able to identify patterns and trends in the data.[12] The amount of data is so large that its effective exploitation cannot rely on traditional human analysis for increased situational awareness. However; the systemic and unsupervised use of AI to process and analyse ever larger sets of data could potentially raise concerns of cognitive bias imported into the analysis – underlining the necessity to keep a human being in the analytical process. Human analysis relies on critical thinking which, so far, has not been perfected in AI-enabled technology.[13]

The Analysis and Manipulation of Personal Data

Combining the data gathered through ISR sensors with personal information gathered from various databases and from social media platforms, could enable the automatic analysis of personally identifiable information by machines. Within the context of NATO Operations, Allies have recognised that capturing and matching biometric samples from individuals encountered in operational theatres could provide a vital capability to support the identification of anonymous operatives to persons, places, items and events, thereby enabling effective, targeted defensive action against threat networks. In the national security and defence field, such calls for greater sharing, while often made, also come up against a wide range of legitimate concerns, including privacy concerns and potential human rights implications.[14] Between North America and Europe, for example, Allies have different national laws with respect to the privacy rights affected by the handling of personal information, including different obligations in international law.

Spoof audio and video

There have been considerable improvements in the production of convincing and high quality virtual reality capabilities.[15] Virtual reality has also become much more accessible in a variety of contexts, for example to optimise museum visits and to support military battlefield training. These technologies can also be used to produce audio and video spoofs, which are used to manipulate the public information space. Not only is the fundamental value of freedom of speech threatened when there is a proliferation of unreliable narratives, but the proliferation of "fake news" introduces doubt and feeds public debate on the factual basis of security related events. In such information environments, government and military decision-making is "slowed" by intense scrutiny on questions of fact: "the existence of widespread AI forgery capabilities will erode social trust, as previously reliable evidence becomes highly uncertain."[16] Virtual reality could also be used to interfere with high-level decision-making, by crippling situational awareness with "fake intelligence", as well as with military command and control, through the introduction of fake orders by an adversary. AI-technology is now even being developed to verify content in order to facilitate the identification of fake, doctored material. As in the two previously mentioned areas, the autonomy of such technologies, independent from human control and oversight, raises the greatest challenge.

A recent Lawfare blog post eloquently stated that, "at this stage of development, AI remains far from intelligent, tending to make mistakes no human would make. Such errors can be unpredictable or difficult to

[12] Ibid. at page 27.

[13] Ibid.

[14] NATO's work in this area builds upon UN Security Council Resolution 2396, S/RES2396 (2017).

[15] For an excellent overview of this area see Allen and Chan, *Supra* note 11.

[16] Ibid. at page 30.

mitigate. In certain cases, the results can be amusing or nonsensical. In a military context, however, there could be adverse consequences".[17] Despite the lack of an international consensus on the definition of AI, the above examples provide some granularity to inform the assessment of the legal implications of the development and use of AI. Drawing from the three areas of AI-enabled technology mentioned above, the term AI-enhanced weapons will be used in the following section in order to capture all uses of AI-enabled weapons, including those focused on systemic disinformation or malicious data manipulation.

4.0 ACCOUNTABILITY OF AI-ENABLED TECHNOLOGY

International and domestic law offers some tools to cope with the effects of AI-enabled weapons from a multinational collective defense perspective. New technology does not necessarily require new laws and it is not the aim of this paper to propose the creation of new legal frameworks. The applicable legal framework will depend on the technology used and on the actual and potential effects caused by that technology and can include various national laws, human rights law, the law of state responsibility, international humanitarian law and the law of armed conflict. With machines taking on the qualities of human intelligence, including perception, cognition and action, the issue of accountability for illegal acts performed by autonomous systems has dominated the debate. The issue is not so much *what* legal framework applies, but *who* is legally responsible for the effects of AI-enabled weapons.

Accountability and Responsibility

AI-enabled action that constitutes an "armed attack" within the sense of Article 51 of the UN Charter, could potentially set off the invocation of Article 5 of the Washington Treaty. Setting aside the issue of the threshold to be applied to determine whether an AI-enabled attack would constitute an "armed attack", the preliminary question that would arise is that of attribution. After all, assigning responsibility for an armed attack is a necessary precondition to the use of self-defence measures. AI-enabled weapons challenge our traditional notions of responsibility: who can be held accountable for the effects of this technology, especially when fully autonomous? Can we even talk of a "legal personality" of AI-enabled systems? In this area, States have been rather clear in expressing the need for responsibility to be attributed to human beings.[18]

The international debates and discussions on the legal approach to take with respect to lethal autonomous weapons systems (LAWS) provides a useful reference on the concept of "human control" where the substance of the debate has been how to regulate human-machine interaction, often referred to as "human-machine teaming". The human role in independent machine decision-making can vary, as exemplified through the OODA loop of decision-making (Observe, Orient, Decide and Act).[19] An "in the loop" system requires human intervention for its operation, an "on the loop" system provides for human intervention if needed, and an "out of the loop" system does not require human intervention at all, a prospect that is criticized by observers who have supported the concept of "minimum human control." Privileging human judgment and accountability above mechanical efficiency, the United States, for example, has taken a clear

[17] E. Kania, "Great Power Competition and the AI Revolution: A Range of Risks to Military and Strategic Stability", 19 September 2017, retrieved from: https://www.lawfareblog.com/great-power-competition-and-ai-revolution-range-risks-military-and-strategic-stability.

[18] See, for example, the reports of the Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects. Reference is made to the *Report of the 2017 Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS)*, CCW/GGE.1/2017/CRP.1 dated 20 November 2017.

[19] P. Tucker, *Tomorrow Soldier: How the Military Is Altering the Limits of Human Performance*, 12 July 2017. Available at: https://www.defenseone.com/technology/2017/07/tomorrow-soldier-how-military-altering-limits-human-performance/139374/.

stance towards asserting that a human being should always be kept in the decision-making loop for the use of LAWS, as the ultimate decider on the use of lethal force in the battlefield.[20]

Human intervention in the OODA loop may be a necessary condition for the application of international humanitarian law to the use of AI-enabled weapons. The rules of international humanitarian law apply to State actors who are behind the planning, the decision-making process and the execution of attacks. The four core principles of necessity, proportionality, discrimination, and humanity, are based on the assumption that human decision-making and judgment underlies military action: "these obligations cannot be delegated or given to machines, a computer program or a weapon system. It is individuals at the end of the day who are responsible for complying with International Humanitarian Law."[21]

The international law of state responsibility can help provide further guidance on the accountability for AI-enabled weapons. Articles 5 to 11 of the International Law Commission's 2001 Articles on Responsibility of States for Internationally Wrongful Acts provide some general principles for determining state responsibility under international law concerning actions of non-state actors, including: close proximity, the exercise of government authority and State direction and control.[22] The rules relating to State Responsibility can inform discussions on defining the relationship and responsibility between human and machine in the use of AI-enhanced weapons.

Legal Personality

Fundamental to the use of AI-enabled technologies are concepts of attribution, breach, and consequences.[23] As noted in a Report from the Global Initiative on Ethics of Autonomous and Intelligence Systems, there was a need to "address the question of how A/IS should be labeled in the courts' eyes: a product that can be bought and sold? A domesticated animal with more rights than a simple piece of property, but less than a human? A person? Something new?" [24]

Witnesses heard for the development of a House of Lord's Report on Artificial Intelligence raised the question of legal personality and underlined that "the decision to award legal status to AI will have many ramifications for legal responsibility and for issues such as legal liability," including for criminal liability. These same witnesses also suggested that without legal personality, "the Government will need to decide

[20] See United States Delegation Closing Statement to 2014 CCW Meeting of Experts on Lethal Autonomous Weapons Systems, 16 May 2014, (audio recording available at UN CCW 2014 LAWS meeting webpage) regarding the assertion that a human being should always be kept in the decision-making loop for the use of AWS noting that the latter "does not sufficiently capture the full range of human activity that takes place in weapon system development, acquisition, fielding and use; including a particular commander's or an operator's judgment to employ a particular weapon to achieve a particular effect on a particular battlefield". The previous statement was found in: K. Neslage, *Does "Meaningful Human Control" Have Potential for the Regulation of Autonomous Weapon Systems?* https://nsac.law.miami.edu/wp-content/uploads/2015/11/Neslage-Final.pdf (Footnote 39).

[21] Interview of the ICRC legal adviser Netta Goussac on the New technologies and IHL, available at: https://www.icrc.org/en/document/icrc-legal-adviser-netta-goussac-talks-about-autonomous-weapons.

[22] C. Mayer, "Developing Autonomous Systems in an Ethical Manner", *in Autonomous Systems: Issues for Defence Policymakers*, published by NATO Allied Command Transformation, ed. Andrew P. Williams and Paul D. Scharre, p. 89.

[23] See D. Lewis, G. Blum, and N. Modirzadeh, *War-Algorithm Accountability*, Harvard Law School Program on International Law and Armed Conflict Research Briefing and Appendices, August 2016. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2832734.

[24] The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems*, Version 2. IEEE, 2017 at page 146. Available at: http://standards. ieee.org/develop/indconn/ec/autonomous_ systems.html.

who takes legal responsibility for these technologies, be it the developers (companies) or the owners". [25] With the complicated legal questions of responsibility and accountability, it is unlikely that States will soon recognize a legal personality for fully autonomous AI-enabled systems. The implications of this are enormous – conveying a legal personality to AI, would be a game changer, further confirming that we are in the throes of an information revolution which will "have implications in multiple domains of human interaction beyond technical issues."[26]

The recent debate on human-machine interaction in the context of AI-enabled weapons has been centered on two basic approaches, the push for further regulation and the push for a ban. Proponents of the "regulate" approach follow the reasoning expressed in the DoD Directive; namely, that regulation is necessary to comply with IHL" [towards allowing] "commanders and operators to exercise appropriate levels of human judgment over the use of force".[27] Supporters of the "ban" approach, such as the NGO Stop Killer Robots, argue that it is unethical to have no human agency in any use of force decisions and that LAWS themselves are inherently unable to comply with IHL requirements. The argument is that given the lack of accountability in IHL for LAWS, these should be banned.

There is some concern regarding the availability of effective remedies for States and individuals injured by the effect of an AI-enabled weapon. Claims under the law of state responsibility may only be brought forward by another State. The same holds true for compensation claims concerning breaches of the law of armed conflict. However, this does not prevent victims of AI-enabled weapons from seeking redress via alternative judicial remedies, for example under international criminal law, which provides for individual responsibility of the perpetrator, including the manufacturer, programmer, or commander, depending on their employment. Concerns about the "accountability gap" in general refer to legal aspects associated with individual accountability not State responsibility, so long as a human being continues to be held accountable for the effects of AI-enhanced autonomous weapons.

Although it may seem premature to anticipate how NATO Allies would react in the event of a serious AI-enabled armed attack, the issue of accountability would have to be addressed by Allies to justify the use of armed force in line with Article 5 of the Washington Treaty. The potential change in the balance of power resulting from States' recent announcements on significant increases in AI research and investments, suggests that such scenarios are not a long way off and could place NATO Allies in the position of providing guidance on these very basic notions of attribution and accountability for AI-enabled systems, with implications across many areas of law.

5.0 CONCLUSION

The aim of this paper is to raise awareness and contribute to a shared understanding of the legal challenges raised by AI-enabled technology, particularly in the context of the international law applicable to collective defence. A primary assumption of this paper is that existing international law provides the appropriate legal framework, but that greater clarity is needed to determine some of the legal debates on how this existing legal framework applies to such new and evolving technologies, especially on the question of accountability. Recognizing that States remain central to the development and the application of international law, NATO,

[25] UK House of Lords Select Committee on Artificial Intelligence Report "AI in the UK: ready, willing and able?" April 16, 2018, at para 437 and 438. Available at: https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf

[26] Supra note 24 at page 148.

[27] See DoD Directive 3000.09, "Autonomy in Weapon Systems", November 21, 2012, available at: https://cryptome.org/dodi/dodd-3000-09.pdf.

as a multinational military organization, can provide a useful forum for the assessment of State practice. From a practical perspective, in order to be effective, a legal baseline should be supported by as many nations as possible. There may also be political value in having an approach with "buy-in" from a number of NATO Allies.

Towards ensuring greater legal preparedness for collective decision making, the NATO legal adviser should have a firm understanding of the legal position of Allies in order to support consensus and effective multinational operations. States are encouraged to make their views known towards increased discussion and interaction. Such interaction would be useful for a variety of reasons, including to identify selected areas where national views and legal obligations amongst Allies may differ. NATO practice should also be recognized as a useful yardstick in areas such as definitions, agreed common frameworks to implement obligations, training programs, and support to international institutions. NATO, as a multinational military organisation relying on legal interoperability, is a useful incubator to draw out elements of State practice.