National Defence
Défense nationale

BORROWING FROM AIRWORTHINESS: HOW TO ACHIEVE MEANINGFUL HUMAN CONTROL IN AUTONOMOUS WEAPON SYSTEMS

Major Keith Fugger

JCSP 46	PCEMI 46
Solo Flight	**Solo Flight**
Disclaimer	**Avertissement**

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 46 – PCEMI 46
2019 – 2020

SOLO FLIGHT

**BORROWING FROM AIRWORTHINESS: HOW TO ACHIEVE
MEANINGFUL HUMAN CONTROL IN AUTONOMOUS WEAPON SYSTEMS**

By Major Keith Fugger

BORROWING FROM AIRWORTHINESS: HOW TO ACHIEVE MEANINGFUL HUMAN CONTROL IN AUTONOMOUS WEAPON SYSTEMS

INTRODUCTION

A new era of warfare is on the horizon. It is based on technology that operates underneath the skin of military equipment, behind closed panels, in little black boxes. It is more than software based on traditional rules; it can learn to recognize and adapt on its own. These learning or cognitive algorithms, based on the premise of artificial intelligence, form the basis of Autonomous Weapon Systems (AWS) and are increasing the level of machine autonomy on the battlefield.

The International Committee of the Red Cross (ICRC) defines an AWS as any weapon system that can "select and attack targets without human intervention."[1] Such weapons are anticipated to bring significant advantages to those who develop and deploy them since they can eliminate human-induced lag, thereby increasing the speed of decision-making and action, reducing risk to own troops, while operating beyond traditional limits of human physiology and in communications-degraded environments.[2]

This technology is also anticipated to proliferate rapidly as algorithms can be easily copied and transferred to various platforms. However, AWS have been the subject of international debate focused on International Humanitarian Law and the ethical problems associated with machines deciding to take human lives.

---

[1] International Committee for the Red Cross, "Autonomous Weapons Could Change the Battlefield of the Future," *New Technologies and IHL*, last accessed 29 April 2020, https://www.icrc.org/en/war-and-law/weapons/ihl-and-new-technologies.

[2] Paul D. Scharre, "1 - The Opportunity and Challenge of Autonomous Systems," *Autonomous Systems – Issues for Defence Policymakers*, The Hague, Netherlands: NATO Communications and Information Agency, n.d., 3-4.

Since 2014, the United Nations Institute for Disarmament Research (UNIDIR) convened meetings of government experts to discuss an internationally accepted path to potentially regulate AWS. UN member states and international organizations, such as the ICRC, were invited to participate in "The Weaponization of Increasingly Autonomous Technologies" project to which Canada donated dedicated funds.[3] UN Secretary General Antonio Guterres described AWS as "politically unacceptable, morally repugnant and should be prohibited by international law."[4] Much of the on-going debate surrounds a concept proposed in a 2013 policy letter from Article36, a non-governmental organization, to the United Kingdom government. In addition to arguing for a ban on fully autonomous weapons, Article36 advocated "a positive obligation in international law for individual attacks to be under meaningful human control."[5] The concept of Meaningful Human Control (MHC) was born, and to this day, continues to frame AWS discussions.

This paper argues that the Department of National Defence (DND) and the Canadian Armed Forces (CAF) Airworthiness policy and framework can be used to meet the intent of MHC and to support the broad use of AWS in operations. The paper begins with more detailed definitions of terms and how Canada and other significant global actors and influencers interpret MHC. The paper will then explain the evolution of MHC in autonomy and introduce some its problems, followed by a description of how risk and a philosophical perspective of guidance control affect the understanding of what MHC

---

[3] United Nations Institute for Disarmament Research, "Current Research - The Weaponization of Increasingly Autonomous Technologies (Phase III)," last accessed 29 April 2020, https://www.unidir.org/projects/weaponization-increasingly-autonomous-technologies-phase-iii-2.

[4] United Nations News, "Autonomous Weapons That Kill Must be Banned, Insists UN Chief," 25 March 2019, https://news.un.org/en/story/2019/03/1035381.

[5] Article36, "Killer Robots: UK Government Policy on Fully Autonomous Weapons," April 2013, last accessed 4 April 2020, http://www.article36.org/wp-content/uploads/2013/04/Policy_Paper1.pdf.

entails. Finally, the paper introduces the DND/CAF Airworthiness framework from which parallels will be drawn to support the generation of an AWS policy inclusive of lethal, fully autonomous systems, meeting the intent of MHC. The ethical basis of using AWS to take human lives is not discussed; the focus is on establishing that an airworthiness-like framework can provide a means to satisfy the concept of MHC.

TERMINOLOGY

Firstly, the ICRC definition of AWS constrains its utility to only those systems that select and attack targets, implying kinetic lethality. Other autonomous systems can 'attack' through other means, with or without lethal effects. Therefore, this paper increases the scope of AWS to include lethal and non-lethal categories that can be treated under a DND/CAF AWS policy. Secondly, Article36 only seeks to apply MHC to individual AWS attacks on humans, implying lethal effects from a direct kinetic attack. Human life, however, can also be taken indirectly, or decidedly preserved through non-lethal means targeting psychological will or through intelligence collection. This broadens application of MHC to weapon systems that do not necessarily conduct kinetic attacks, as their development and implementation will experience similar issues but might not pose as significant of risks.[6]

This paper uses the following CAF definition for targeting: "the process of identifying, selecting and prioritizing targets to produce physical or behavioural effects."[7] Notice there is no explicit mention of attack. In this context, targeting is associated with

---

[6] The CAF considers aircraft such as the CC130J Hercules as a weapon system even though it does not conduct attacks.

[7] Government of Canada, Termium Plus "Targeting", Record 1, 1 October 2019, https://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&i=1&srchtxt=targeting&codom2nd_wet=1#resultrecs.

a larger set of effects in the battlespace, not just physical attack. This permits the use of AWS in the information and cyber domains (e.g. targeting key populations with a specific narrative or targeting physical entities through virtual means which might include attacking). In consolidating the above, AWS can be either lethal or non-lethal, and used to deliver effects (including through targeting) in the operating environment without human intervention. Although the broader definition might not align with the original intent of MHC, it is how the DND/CAF should approach its application to AWS through policy and supporting framework.

Finally, the notion of autonomy can be vague. The CAF defines autonomy as:

A system's ability to function, within parameters established by programming and without outside intervention, in accordance with desired goals, based on acquired knowledge and an evolving situational awareness.[8]

The degree to which a system has the aforementioned ability dictates the system's level of autonomy. As there can be various levels of autonomy, a system can be said to occupy a particular place on the autonomy spectrum, from those with minimal autonomy that require constant manual manipulation to those that are fully autonomous. The proposed ban on AWS is for those that are fully autonomous. The concept of MHC can apply to all AWS across the spectrum. As autonomy increases, the level of 'human control' can be said to decrease yet remain 'meaningful.'

---

[8] *Ibid*., "Autonomy", Record 2, 12 September 2019, https://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&i=1&srchtxt=autonomy&codom2nd_wet=1#resultrecs.

PERSPECTIVES ON MEANINGFUL HUMAN CONTROL

International

The United Nations' *1980 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* has 125 State Parties.[9] It is under this convention that government experts discuss AWS potential definitions, purposes, classifications, regulation and ban, as well as refining the concept of MHC. As of September 2019, only 29 nations support the ban on lethal AWS.[10] Canada, the United States (US), and the Russian Federation (Russia), although participants in the international discussions, are among those that do not formally support the ban. China only supports a ban on the operational use of AWS, not on their development. As an indication of the increasing desire for AWS around the world, global investment in military robotics increased from US$2.4 billion in 2000 to US$7.5 billion in 2015, and is anticipated to grow to US$16.5 billion by 2025.[11] A significant portion of the investments finance development of AWS underlying technology: artificial intelligence. The following paragraphs describes the ambitions of Russia, China, the US and Canada, as well as how they interpret MHC.

Russia

Russia supports the informal UNIDIR discussions regarding AWS and the concept of MHC, but does not support an outright ban on lethal AWS.[12] Aside from the

---

[9] United Nations News, "Autonomous Weapons That Kill Must be Banned, Insists UN Chief," 25 March 2019, https://news.un.org/en/story/2019/03/1035381.

[10] Human Rights Watch News, "'Killer Robots:' Ban Treaty Is the Only Credible Solution," 26 September 19, https://www.hrw.org/news/2019/09/26/killer-robots-ban-treaty-only-credible-solution.

[11] Meldon Wolfgang *et al*, "Gaining Robotics Advantage," Boston Consulting Group, 14 June 2017, https://www.bcg.com/publications/2017/strategy-technology-digital-gaining-robotics-advantage.aspx.

[12] The Russian Federation, *Examination of various dimensions of emerging technologies in the area of lethal autonomous weapons systems, in the context of the objectives and purposes of the Convention*, Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions

discussions failing to achieve consensus on definitions and no apparent working form of lethal, fully-autonomous weapon system to use as an example, Russia believes that a "clear distinction between civilian and military developments of autonomous systems based on the same technologies is still an essential obstacle" in moving forward.[13] The Federation aims to have AWS on the battlefield by 2025 in the form of multifunctional robots, some with lethal capabilities.[14] Russia is expected to continue participating in international AWS discussions while developing operational systems. However, Russian Security Council Secretary Nikolai Patrushev compared AWS with weapons of mass destruction, conceding that the international community should quickly develop "a comprehensive regulatory framework" preventing use of advanced technologies that undermine national and international security.[15] The Russian government might have a genuine interest in regulating AWS or it might be another political ploy to keep the international community questioning Russian motives.

China

The Central Military Commission seeks to monopolize on the revolution in intelligent technologies[16] as China aims to become the world leader in artificial intelligence by 2030.[17] According to the Communist Party, this is not without its

on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, 10 November 2017, 1.

[13] *Ibid*., 2.

[14] Igor Rozin, "Russia to create first unit of battle robots by mid-2020s," Russia Beyond, 29 November 2019, https://www.rbth.com/science-and-tech/331349-russia-to-create-first-robots.

[15] Samuel Bendett, "Did Russia Just Concede a Need to Regulate Military AI?", Defense One, 25 April 2019, https://www.defenseone.com/ideas/2019/04/russian-military-finally-calling-ethics-artificial-intelligence/156553/.

[16] Wilkie Briggs, "Is China's Interest In Autonomous Weapons Cause For Concern?", AI Business, last accessed 2 May 2020, https://aibusiness.com/is-chinas-interest-in-autonomous-weapons-cause-for-concern/.

[17] State Council of China, *State Council on Issuing Notification of New Generation Artificial Intelligence Development Planning*, 20 July 2017, http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.

challenges, such as laws, regulations and ethics to safeguard healthy and rapid development of these technologies. Their national strategy emphasizes human-machine collaboration, but does not explicitly discuss MHC.[18] China's international position supports further refinement of the MHC concept and detailed AWS reviews under International Humanitarian Law.[19] However, the nature of the communist regime suggests their interpretation of appropriate safeguards might be different than western democracies, and so China "may be more willing to relinquish 'meaningful human control' in order to achieve ever-greater cognitive speed in battlefield actions."[20] Although China supports a ban on the use of AWS, the international community must not be swayed to think that China will never use them once developed, turning a blind eye to proposed safeguards such as MHC to achieve their goals.

The United States

There is no restriction in US policy regarding the development and implementation of AWS, lethal or non-lethal. The US government opposes an international ban, and posits that lethal AWS should be developed and implemented as they would "increase the ability of States to reduce the risk of civilian casualties in applying force" based on their increased accuracy and precision.[21] The US Department of

---

[18] *Ibid.*.

[19] People's Republic of China, *Position Paper*, 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, 11 April 2018, 1-2.

[20] Stephen De Spiegeleire, Matthijs Maas and Tim Sweijs, *Artificial Intelligence and the Future of Defense – Strategic Implications for Small- and Medium-sized Force Providers*, (The Hague, NE: The Hague Centre for Strategic Studies, 2017), 80.

[21] Charles Turnbull (U.S. Mission to International Organizations in Geneva), Speech, U.S. Statement on LAWS: Potential Military Applications of Advanced Technology, First Session of the Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS), Geneva, 25 March 2019, https://geneva.usmission.gov/2019/03/26/u-s-statement-on-laws-potential-military-applications-of-advanced-technology/.

Defense (DOD) Directive on lethal AWS adapted the concept of MHC to meet national

interests, stating that all systems must "allow commanders and operators to exercise

appropriate levels of human judgment over the use of force."[22] The term 'appropriate'

implies flexibility as the level of judgment necessary may be situationally dependent. The

term 'judgment' replaces 'control,' allowing a human to initiate the system depending on

the operational context and considering international law, the particular rules of

engagement, and the system's capabilities and limitations. Under the same directive,

lethal AWS are required to undergo a senior review within the DOD, in addition to the

normal weapon review process, before development and again before acceptance into

service.

Canada

Canada remains committed to the international discussions of government experts

on AWS at the UN since "an open and collaborative dialogue … will help shape

international conversations and policy development."[23] Although Canada has not signed

onto the ban on fully autonomous lethal weapon systems internationally, at the national

level, Prime Minister Justin Trudeau directed the Minister of Foreign Affairs, the

Honourable François-Philippe Champagne, to "advance international efforts to ban the

development and use of fully autonomous weapons systems."[24] Therefore, Canada does

not oppose the ban like the US and could become more vocal in the international

---

[22] Congressional Research Service, *Defense Primer: U.S. Policy on Lethal Autonomous Weapon Systems*, last modified 19 December 2019, https://fas.org/sgp/crs/natsec/IF11150.pdf.

[23] Rosemary McCarney (General Debate opening remarks), CCW States Parties Group of Governmental Experts on Lethal Autonomous Systems (LAWS), Geneva, Switzerland, 9-13 April 2018, https://www.unog.ch/80256EDD006B8954/(httpAssets)/86612887B010EB33C12582720056F0C6/$file/2018_LAWSGeneralExchange_Canada.pdf.

[24] Prime Minister of Canada, *Minister of Foreign Affairs Mandate Letter* (Ottawa: Office of the Prime Minister, 13 December 2019), https://pm.gc.ca/en/mandate-letters/2019/12/13/minister-foreign-affairs-mandate-letter.

community. DND was fortunate to have Dr. Simon Monckton, a leading defence scientist on unmanned systems, participate in the Canadian delegation headed by Ms. Rosemary McCarney, Ambassador and Permanent Representative to the United Nations and the Conference on Disarmament. However, compared to other delegations, Canada did not include military members.[25]

Canada's defence policy, *Strong, Secure, Engaged*, describes the government's position regarding advanced military capabilities: these systems will be developed and implemented in such a way that "respects all applicable domestic and international law, is subject to proven checks and balances, and ensures full oversight and accountability."[26] Similar to the US interpretation of MHC, Canada has decided not to explicitly state 'meaningful human control' in its defence policy; yet, it remains "committed to maintaining appropriate human involvement in the use of military capabilities that can exert lethal force."[27] The level of appropriateness and how the human is involved remains to be to defined, and depends on the operational context. This paper proposes such a framework building on MHC research and based on airworthiness policy principles.

EVOLUTION OF MEANINGFUL HUMAN CONTROL IN AUTONOMY

The concept of MHC is quite simple since it is written using common vocabulary. It qualifies the type of control as 'meaningful' and emphasizes human involvement,

---

[25] The US, France, Croatia and the UK are some countries that sent military officers as part of their past delegations. The list of participants to the 2019 meetings in Geneva is found at https://www.unog.ch/80256EDD006B8954/(httpAssets)/3DBF4443C79AC6ABC12584BE004565B4/$file/CCW+GGE.1+2019+INF.1+Rev.1.pdf.

[26] Department of National Defence. *Strong, Secure, Engaged – Canada's Defence Policy* (Ottawa: DND Canada, 2017), 55.

[27] *Ibid*., 73.

responsibility and accountability, also known as human agency.[28] However, what is meaningful for one person might not be the same as for someone else, let alone for one state compared to another. In addition to the various interpretations of 'meaningful,' how much human control is necessary to be 'meaningful' might vary as well from person to person and from state to state. Already, Canada and the US avoid the terms 'meaningful' and 'control' in their respective policy documents. Article36's concept of MHC "provides an approach… not a solution."[29]

In 2016, in response to the identified interpretation issues above, Article36 developed the six principles below to refine the concept of MHC focusing on the underlying AWS technology, the user, and processes.[30] For an AWS to meet the intent of MHC:

1. The technology must be predictable within certain parameters and within a system of systems;

2. The technology must be reliable based on inherent design and allows graceful performance degradation;

3. The technology must be transparent so a human can understand system reasoning, goals, and constraints;

---

[28] United Nations Institute for Disarmament Research, *The Weaponization of Increasingly Autonomous Technologies: Considering How Meaningful Human Control Might Move the Discussion Forward*, Geneva: UNIDIR, 2014, 3.
[29] *Ibid.*, 4.
[30] Heather M. Roff and Richard Moyes, *Meaningful Human Control, Artificial Intelligence and Autonomous Weapons*, Briefing paper prepared for the Informal Meeting of Experts on Lethal Autonomous Weapons Systems, UN Convention on Certain Conventional Weapons, April 2016 (London: Article36, 2016), 2-3.

4. The user must have accurate information of the technical system functioning, the parameters in which it functions, the desired effects of its use, and the situation at hand; as well the user must have confidence in that information;

5. There must be timely human action and a capacity for timely intervention such that a human initiates the system when relevant to do so and the system accepts intervention from another machine or a human based on feedback cues; and

6. There must be accountability to a certain standard so humans understand they are responsible and accountable for initiating the system processes and the consequences of their actions or inactions in their role within the system.

These principles indicate that the original intent of establishing MHC over individual attacks on humans has matured into a more holistic approach of MHC over the entire weapon system. However, they introduce new questions regarding how predictable, reliable, and transparent the system must be, how accurate the information needs to be, how much confidence the user must have in the information, and how timely actions must occur. This paper suggests that the answer to those questions depend on the situation in which an AWS is intended to be used. Hardly a definitive and quantifiable answer, but one that allows further exploration of these principles, the intent of MHC, risk in the discussion below, and later on, how the DND/CAF airworthiness framework can apply. The operational context was also adopted by the US in its AWS policy by using the term 'judgment' instead of 'control', promoting the use of human judgment based on the operational context. The same could be said for Canada: 'appropriate human involvement' to meet the particular operational need in a particular situation.

The Role of Risk

Uncertainty encapsulates warfare (i.e. the fog of war); the aim is to be as certain as possible given the information and situation at any given moment to make the best decision possible in achieving the desired outcomes. As with any weapon system, there "will be a moment after which control is lost over the direct outcome."[31] Therefore, there is inherent risk in not achieving the desired outcome and is dependent on the operational context. The concept of MHC intends to reduce the uncertainty associated with AWS use.

Michael C. Horowitz and Paul Scharre, Fellows at the Center for a New American Security, claim MHC consists of three essential components to ensure AWS do not pose unacceptable risk:[32]

1. Human operators making informed, conscious decisions about the use of weapons;

2. Human operators have sufficient information to ensure lawfulness of action they direct given details regarding targets, weapons, and context for action; and

3. Weapon is designed and tested, and human operators are properly trained to ensure effective control over the use of the weapon system.

Firstly, humans involved in AWS operations must not make arbitrary decisions to use them, but they must understand the functioning of the system, its interaction with the operating environment, and how their decision to use AWS can affect that environment.

---

[31] Mark Roorda, "NATO's Targeting Process: Ensuring Human Control Over (and Lawful Use of) 'Autonomous' Weapons," *Autonomous Systems – Issues for Defence Policymakers*, The Hague, Netherlands: NATO Communications and Information Agency, n.d., 161.

[32] Michael C. Horowitz and Paul D. Scharre, *Meaningful Human Control in Weapon Systems: A Primer* (Washington, D.C.: Center for a New American Security, 2015), 4, https://www.cnas.org/publications/reports/meaningful-human-control-in-weapon-systems-a-primer.

Above all, humans must be aware of the consequences of their decision, and then decide to act.

Secondly, operators and commanders cannot have a complete appreciation and understanding of a situation, especially in warfighting. The humans in the chain of command must therefore analyze the situation before determining if an AWS action (or behaviour) poses acceptable or unacceptable risk. Considering the dynamic nature of the operating environment and the learning ability of cognitive systems behind AWS technology, this analysis might have to be performed often.

Thirdly, technical performance of the system must be proven to meet specific criteria and human-centred system training must be sufficient to satisfy the requirements of the previous two components. These three MHC essentials align with the intent of the six principles put forward by Article36, but they do not define what 'effective control' means nor is there a consideration of human intervention. They do, however, bring up the concept of risk, and how risk management can help humans to decide whether to use the AWS in a particular situation.

Lastly, maintaining 'effective control,' as Scharre independently clarified, consists of accurately predicting AWS behaviour and the ability of a human to intervene if the system does not behave in accordance with the desired intent.[33] A failure is therefore defined as a loss of 'effective control,' and the risk of failure is based on the probability and consequences of such a loss. This too is context dependent. Just because the risk of failure might be significant does not necessarily mean that the risk is

---

[33] Paul D. Scharre, *Autonomous Weapons and Operational Risk* (Washington, D.C.: Center for a New American Security, 2016), 8, https://www.cnas.org/publications/reports/autonomous-weapons-and-operational-risk.

unacceptable. The chain of command should determine what risk is acceptable in a given situation; what might be acceptable in one situation might not be in another. Any organization that operates AWS must inculcate "a culture that emphasizes human responsibility."[34] Formal risk acceptance authority within the chain of command supports such a culture.

Role of Guidance Control Philosophy

Responsibility and accountability for the use of AWS and their associated behaviours are recurring themes in the ongoing debate on their ethical use. Using Fischer and Ravizza's philosophical theory of guidance control, Filippo Santoni de Sio and Jeroen van den Hoven establish conditions under which an AWS, as part of a (life and death) decision-making cycle, can remain under MHC:[35]

1. The system must be able to track relevant human moral reasons regardless of the separation between the human and the system in question; and

2. The system's actions must be traceable to a moral understanding of at least one human associated with its design, programming, or operation, where that person understands the system's capabilities and the potential consequences of its use and is also aware that others might have a moral reaction towards them.

In other words, the control is not meaningful unless the AWS can track the moral intent of the 'controlling' human, and its actions can be traced back to a human that occupies a position in "a recognized social or legal architecture of duties and

---

[34] *Ibid.*, 44.

[35] Filippo Santoni de Sio and Jeroen van den Hoven, "Meaningful Human Control over Autonomous Systems: A Philosophical Account," Frontiers in Robotics and AI 5, no. 15 (February 2018): 1, https://www.frontiersin.org/articles/10.3389/frobt.2018.00015/full.

responsibilities" behind its development or operation.[36] Thus, in addition to the

technological capabilities the AWS must demonstrate, humans within an accepted system

of rules, processes and standards are a critical component of establishing MHC and in

reducing the risk of creating responsibility and accountability gaps. The DND/CAF

airworthiness framework is a good example of architecture from which an AWS policy

can be drafted: it ensures human involvement using an formal and accepted architecture

of duties and responsibilities, including risk acceptance and training, to develop and use

advanced technologies that can take human lives.

MEANINGFUL HUMAN CONTROL AND AIRWORTHINESS

Introduction to DND/CAF Airworthiness

Before showing how airworthiness principles apply to the concept of MHC over

AWS regardless of domain, one must first understand the institutional governance and

purpose of airworthiness. Departmental policy is provided by *Defence Administrative*

Order and Direction (DAOD) 2015-0, Airworthiness issued under Ministerial Direction

that is subordinate to federal legislation, the *Aeronautics Act*.[37] The DND/CAF

airworthiness policy statement outlines its purpose: "The DND and the CAF are

committed to achieving and maintaining an acceptable level of safety for military

aviation."[38] The key phrase is 'acceptable level of safety,' which is found throughout

subordinate documentation and aligns with civilian aviation safety measures. Ministerial

responsibilities are delegated to the Chief of the Defence Staff (CDS) who, in turn,

designates the Commander of the Royal Canadian Air Force (Comd RCAF) as the

---

[36] *Ibid.*, 10.

[37] Department of National Defence, *DAOD 2015-0 Airworthiness*, (Ottawa: DND Canada), last modified 26 July 2018.

[38] *Ibid.*.

Airworthiness Authority for the DND/CAF, responsible for "overall supervision and management of the [mandated] airworthiness program."[39]

The airworthiness program is described in *DAOD 2015-1, DND/CAF Airworthiness Program*, and governs the design, manufacture, maintenance, materiel support and operation of military aeronautical products. The aim of the program is "to ensure that an acceptable level of aviation safety is achieved and maintained for military aviation."[40] The program provides a framework for the regulation of aviation activities, outlines positions of authority and the risk management process, and stipulates that only qualified and competent individuals can be authorized to perform airworthiness activities.

The CDS designates a Technical Airworthiness Authority (responsible for design, manufacture and maintenance/support aspects) and an Operational Airworthiness Authority (responsible for flight operations, aerospace control, standards and training, and personnel to name a few) as shown in Figure 1 below.[41] Both authorities are further responsible for independent airworthiness programs within their technical or operational domains and are subordinate to the overall Airworthiness Authority (Comd RCAF). These Airworthiness authorities, as well as the Investigative Authority (which investigates when something goes wrong), are delegated Ministerial authorities stemming from the *Aeronautics Act*.[42] To ensure initial and continued airworthiness of aeronautical products and that key leaders remain engaged, the program mandates separate Airworthiness Review Boards and Airworthiness Advisory Boards held at regular

---

[39] *Ibid.*.

[40] Department of National Defence, *DAOD 2015-1 DND/CAF Airworthiness Program*, (Ottawa: DND Canada), last modified 26 July 2018.

[41] Department of National Defence, A-GA-005-000/AG-001, *Department of National Defence / Canadian Armed Forces Airworthiness Program*, (Ottawa: DND Canada, 2020), 1-1-10.

[42] *Ibid.*, 1-2-3.

intervals. Each of the designated authorities are formally delegated responsibilities, including to accept specific levels of risk.
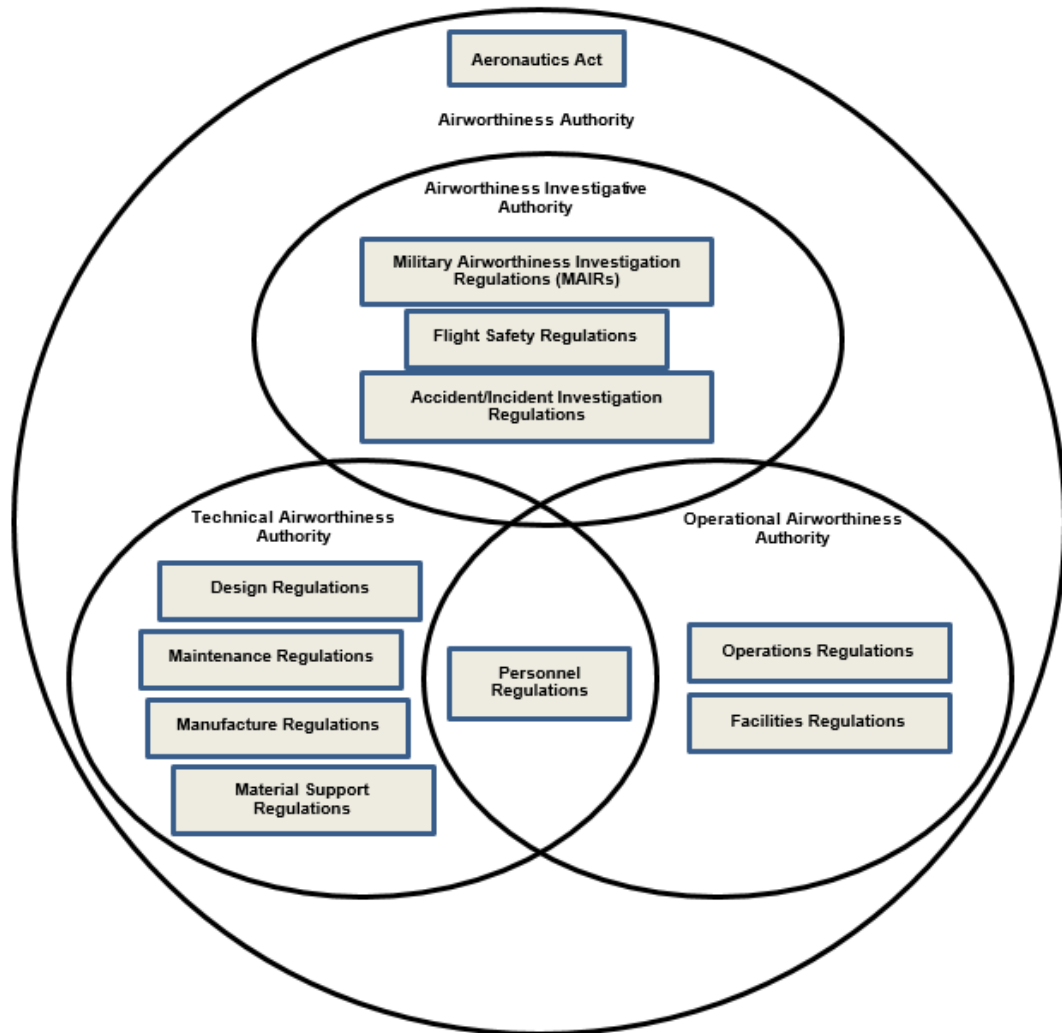

Figure 1 – DND/CAF Airworthiness Management Framework

The *DND/CAF Airworthiness Program Manual* contains the program's fundamental principles, ensuring airworthiness-related activities are:[43]

1. Completed to accepted standards;

2. Performed by authorized individuals;

---

[43] *Ibid.*, 1-1-5.

3. Accomplished within accredited organizations; and

4. Done using approved procedures.

These principles direct the development of appropriate training for personnel, the standards those personnel must achieve to become authorized to perform airworthiness-related activities, the procedures used in performing those activities, and organizational requirements to ensure continued quality work performed by competent individuals. This sounds like a rigid institutional architecture, but through the concept of 'Primacy of Operations' commanders can balance "mission accomplishment demands against aviation safety goals."[44] Any reduction in safety must be documented and accepted by a competent authority, normally through the completion of a risk assessment relevant to the situation faced. Lastly, to ensure continued compliance with desired behaviours over time, personnel, equipment and processes are verified, audited, tested and results compared to accepted standards and regulations. The airworthiness program is human-centred, operations focused, and contains checks and balances to ensure continued acceptable levels safety, a framework applicable to AWS in any domain.

Borrowing from Airworthiness to Achieve Meaningful Human Control

The DND/CAF AWS policy statement should emphasize the commitment to achieving and maintaining an acceptable level of MHC and safety in AWS. The policy should be subordinate to government direction[45] and mandate implementation of an AWS-MHC program. The policy should have the CDS designate an AWS authority in

---

[44] *Ibid.*, 1-1-13.

[45] For example, Minister of National Defence Direction if no federal legislation is enacted regarding safe use of autonomous systems in general. Autonomous systems are not only applicable to national defence but are more commonly found across commercial industry. Cognitive algorithms can serve a dual-purpose, civilian and military, with only the latter associated with weapon systems.

the CAF, a military flag officer, responsible for overall supervision and management of an AWS-MHC program across the DND/CAF covering lethal and non-lethal AWS. Since authorities already exist for particular platforms, such as aircraft, ships, submarines and land vehicles, the AWS Authority is limited to only the cognitive aspects of the platform and not over the host platform itself.[46] Lastly, the policy should require DND and CAF personnel to perform AWS-related activities in accordance with the AWS-MHC program and any legislation as directed by government.

The DND/CAF AWS-MHC program must govern the design, programming, maintenance and operation of AWS cognitive algorithms. The aim of the program should be to ensure that an acceptable level of safety and MHC are achieved and maintained for AWS operations. The program will provide a framework for the regulation of AWS in the DND/CAF and outline additional authorities designated by the CDS, such as a Technical Authority and an Operational Authority, as well as their associated responsibilities. AWS exploit a specialized technical field, artificial intelligence, in which few military personnel have the opportunity to excel. Moreover, the turnover of military personnel in technical positions is difficult to sustain once expertise is developed. Therefore, the Technical Authority should be a civilian responsible for ascertaining and maintaining the technical performance of AWS algorithms and for a Technical AWS-MHC Program. The Technical Authority ensures that the AWS cognitive algorithm was 'built right.' This authority could reside with the Associate Deputy Minister (Information

---

[46] Programs are already in place for air, maritime surface and subsurface, and land vehicle platforms within their respective domains. These programs should not be duplicated for AWS; therefore, AWS authorities must govern the cognitive aspects of the platform contained in the algorithms specifically.

Management) (ADM(IM)) or ADM (Data, Innovation and Analytics) due to the technological expertise within their respective branches.[47]

The Operational Authorities should be military flag officers responsible for the operational use of AWS algorithms and platforms within their domain, and for an Operational AWS-MHC Program. The Operational Authorities ensure the AWS platform built, including algorithm, was 'the right thing' and satisfies operational requirements. The CDS could designate a number of Operational authorities, perhaps four: one under each of the Comd Royal Canadian Navy, Comd Army, Comd RCAF, and Comd Special Operations Forces Command, responsible for the operational use of AWS within their traditional domains. An additional fifth Operational Authority could reside with Comd CJOC for Information Operations and Cyber AWS.[48] The Operational Authorities must have a close relationship with the Technical Authority to resolve issues and to keep one another apprised of changing operational requirements.

The above paragraphs describe a formal structure of authorities, responsibilities and accountabilities as well as distinct human involvement in the technical and operational aspects of AWS development and operations. Issues such as reliability, predictability and transparency could be measures for the Technical Authority to determine, while AWS training for specific personnel in the user chain as well as the degree to which an AWS can perform a mission as intended are issues for the Operational Authority to manage. Cognitive algorithm modification, validation, and verification will

---

[47] The Technical Authority and formal delegates can accept technical risk for AWS algorithms, but not operational risk.

[48] Comd CJOC is responsible for information operations under the CAF Targeting Initiative, but cyber capabilities are an ADM(IM) responsibility, a technical, non-military position. The decision to accept operational risk within a domain should reside with a military flag officer in the military chain of command.

play critical roles throughout the life of an AWS, as will test and evaluation of the AWS within the larger CAF system-of-systems approach.[49] The degree to which AWS can be expected to meet technical and operational requirements can be assessed and the results submitted to the appropriate authorities for acceptance into service.

AWS, by their very nature, can learn from the external environment and might not be at the same baseline of safety after a mission as it was before. In these instances risk management "provides military decision-makers with a logical and systematic framework" that allows them to assess the risk of using an AWS against the military benefit even if there is no human directly controlling the system's every action.[50] The risk assessment process has particular inputs for each hazard, including probability, impact (or consequence), mitigating procedures (to avoid a hazard situation), and corrective actions (if the hazard is encountered). Risks can be either technical or operational, and must only be accepted by those formally delegated proper authorities in accordance with the AWS-MHC program. Operational commanders must be given the flexibility to balance the needs of AWS safety with accomplishing military objectives, understanding the risks and possible consequences of the systems actions. Although the risk of using an AWS in a particular context might be extremely high, the military advantage and benefit might outweigh the risk, resulting in the risk's formal acceptance by a human commander with the authority to accept extremely high risk for AWS.

The notion of risk in lethal AWS operation is fairly evident considering the amount of debate regarding machines taking human lives and ensuring only those

---

[49] Department of National Defence, *Strong, Secure, Engaged – Canada's Defence Policy* (Ottawa: DND Canada, 2017), 70.
[50] *Ibid.*, 2-2-1.

intended will be attacked. However, non-lethal AWS can also be treated using the same policy and framework discussed above to guarantee MHC. An autonomous Search and Rescue vehicle, whether in the air, on or under the sea surface, or on the ground, can be used to locate and assist persons in distress. These vehicles must also perform as intended and not focus attention on false targets. In this case, the risk is not in identifying and attacking the wrong targets but in identifying and assisting the wrong targets. This could lead to people unnecessarily dying. The development, programming, maintenance, operation and personnel training for such non-lethal AWS must also conform to accepted processes and standards within a framework of responsibility and accountability. The same can be applied to autonomous cyber weapon systems; however, the cyber domain is relatively new and further investigation is necessary to determine the most suitable application of an AWS-MHC program to cyber operations.

CONCLUSION

AWS, both lethal and non-lethal, are expected to bring increased speed, range and endurance across all domains in the future battlespace. Some nations, like the US, claim these weapon systems will also increase accuracy and reduce collateral damage during attacks, and therefore, must be developed and implemented. The promise of military advantages, however, is being weighed against International Humanitarian Law and the ethics of machines deciding to take human lives without direct human intervention. The concept of MHC is one approach being discussed at the international level to ensure humans retain responsibility for actions and behaviours of AWS, and as described above, not only during attack but in performing various tasks as intended by the chain of

command. Attacks are the main focus, but not the only one, since they pose the greatest risk to innocent human life.

Autonomy can be viewed as a spectrum, and as autonomy increases, the level of human involvement decreases. How 'meaningful' the control might be and how much control is required to be 'meaningful' are not well defined, and can vary from state to state and from one operational situation to another. The level of MHC will depend on the technological capabilities of the AWS and on the operational context in which it might be used: the operating environment, human knowledge of AWS functioning, and the potential consequences in its use. Canada decided to substitute MHC with 'appropriate human involvement' but the intent remains unchanged: to prevent undesirable outcomes.

To have any credibility and legitimacy at home and internationally, the DND/CAF must have a policy and framework in place which emphasizes human responsibility and accountability for mission outcomes including those resulting from AWS. The DND/CAF Airworthiness Program provides just that to ensure an acceptable level of safety in military aviation: a structure of human decision-makers with specific authorities and responsibilities, and traceable processes that support decision-making, risk acceptance, as well as development, maintenance, operations and training. Borrowing from airworthiness, the DND/CAF policy and framework for AWS must emphasize MHC and an acceptable level of safety in AWS development and implementation. Independent Technical and Operational Authorities will minimize groupthink, and separate technical algorithmic issues from operational ones that impact the AWS as a whole and its place within the CAF system-of-systems. Operational commanders, however, must be able to balance achieving military objectives using AWS

against safety, and to accept the consequences of their decision. The risk management process, as well as others, supports the intent of MHC.

The AWS-MHC Program must ensure that AWS-related activities (development, programming, maintenance, training, operations and oversight) are completed to accepted standards, performed by authorized individuals (military and civilian), accomplished within accredited organizations (military and civilian), and done using approved procedures. Due to the rapid pace of technological change and the learning aspect of AWS algorithms, the AWS-MHC Program will need to be managed more closely than for military aviation.

Policy discussions, which will inform the program, "will need to be primarily a social and political process and not merely – or even primarily – a technical and legal exercise."[51] The military institution alone should not determine AWS policy. Considering the nature of the debate, Government, industry, and society involvement is necessary not only at the international level but domestically as well.

---

[51] United Nations Institute for Disarmament Research, *The Weaponization of Increasingly Autonomous Technologies: Considering How Meaningful Human Control Might Move the Discussion Forward* (Geneva: UNIDIR, 2014), 9.

BIBLIOGRAPHY

Article36. "Killer Robots: UK Government Policy on Fully Autonomous Weapons." April 2013. Last accessed 4 April 2020. http://www.article36.org/wp-content/uploads/2013/04/Policy_Paper1.pdf.

Bendett, Samuel. "Did Russia Just Concede a Need to Regulate Military AI?" Defense One. 25 April 2019. https://www.defenseone.com/ideas/2019/04/russian-military-finally-calling-ethics-artificial-intelligence/156553/.

Briggs, Wilkie. "Is China's Interest In Autonomous Weapons Cause For Concern?" AI Business. Last accessed 2 May 2020. https://aibusiness.com/is-chinas-interest-in-autonomous-weapons-cause-for-concern/.

Canada. Department of National Defence. A-GA-005-000/AG-001, *Department of National Defence / Canadian Armed Forces Airworthiness Program*. Ottawa: DND Canada, 2020.

Canada. Department of National Defence. *DAOD 2015-0 Airworthiness*. Ottawa: DND Canada, 26 July 2018.

Canada. Department of National Defence. *DAOD 2015-1 DND/CAF Airworthiness Program*. Ottawa: DND Canada, 26 July 2018.

Canada. Department of National Defence. *Defence Information Strategy*. Ottawa: DND Canada, 2019.

Canada. Department of National Defence. *Strong, Secure, Engaged – Canada's Defence Policy*. Ottawa: DND Canada, 2017.

Canada. Department of National Defence. *The Department of National Defence and Canadian Armed Forces Data Strategy*. Ottawa: DND Canada, 2019.

Canada. Government of Canada. Termium Plus "Autonomy." Record 2. 12 September 2019. https://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&i=1&srchtxt=autonomy&codom2nd_wet=1#resultrecs.

Canada. Government of Canada. Termium Plus "Targeting." Record 1. 1 October 2019. https://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&i=1&srchtxt=targeting&codom2nd_wet=1#resultrecs.

Canada. The Prime Minister of Canada. *Minister of Foreign Affairs Mandate Letter*. Ottawa: Office of the Prime Minister, 13 December 2019. https://pm.gc.ca/en/mandate-letters/2019/12/13/minister-foreign-affairs-mandate-letter.

Horowitz, Michael C. and Paul D. Scharre. *Meaningful Human Control in Weapon Systems: A Primer*. Washington, D.C.: Center for a New American Security, 2015. Last accessed 4 April 2020. https://www.cnas.org/publications/reports/meaningful-human-control-in-weapon-systems-a-primer.

Human Rights Watch News. "'Killer Robots:' Ban Treaty Is the Only Credible Solution," 26 September 19. https://www.hrw.org/news/2019/09/26/killer-robots-ban-treaty-only-credible-solution.

International Committee for the Red Cross. "Autonomous Weapons Could Change the Battlefield of the Future." New Technologies and IHL. Last accessed 29 April 2020. https://www.icrc.org/en/war-and-law/weapons/ihl-and-new-technologies.

International Committee for the Red Cross. "Autonomous Weapons: States Must Agree on What Human Control Means in Practice." 20 November 2018. https://www.icrc.org/en/document/autonomous-weapons-states-must-agree-what-human-control-means-practice.

International Committee for the Red Cross. Views of the International Committee of the Red Cross (ICRC) on Autonomous Weapon Systems. Convention on Certain Conventional Weapons (CCW) Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS) 11-15 April 2016, Geneva. 11 April 2016. https://www.icrc.org/en/download/file/21606/ccw-autonomous-weapons-icrc-april-2016.pdf.

Keeley, Thomas. "Auditable Policies for Autonomous Systems (Decisional Forensics)." *Autonomous Systems – Issues for Defence Policymakers*, 196-222. The Hague, Netherlands: NATO Communications and Information Agency, n.d.. https://www.act.nato.int/images/stories/media/capdev/capdev_02.pdf.

McCarney, Rosemary. General Debate opening remarks. CCW States Parties Group of Governmental Experts on Lethal Autonomous Systems (LAWS), Geneva, Switzerland, 9-13 April 2018. Last accessed 4 May 2020. https://www.unog.ch/80256EDD006B8954/(httpAssets)/86612887B010EB33C12582720056F0C6/$file/2018_LAWSGeneralExchange_Canada.pdf.

Moyes, Richard. *Autonomy in Weapons Systems – Considering Approaches to Regulation*. Article36. March 2020. http://www.article36.org/wp-content/uploads/2020/03/Regulation-approaches-Mar-2020.pdf.

People's Republic of China. *Position Paper*. 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, 11 April 2018. https://unog.ch/80256EDD006B8954/(httpAssets)/E42AE83BDB3525D0C125826C0040B262/$file/CCW_GGE.1_2018_WP.7.pdf.

People's Republic of China. State Council of China. *State Council on Issuing Notification of New Generation Artificial Intelligence Development Planning*. 20 July 2017, http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.

Roff, Heather M. and Richard Moyes. *Meaningful Human Control, Artificial Intelligence and Autonomous Weapons*. Briefing paper prepared for the Informal Meeting of Experts on Lethal Autonomous Weapons Systems, UN Convention on Certain Conventional Weapons, April 2016 (London: Article36, 2016). http://www.article36.org/wp-content/uploads/2016/04/MHC-AI-and-AWS-FINAL.pdf.

Roorda, Mark. "NATO's Targeting Process: Ensuring Human Control Over (and Lawful Use of) 'Autonomous' Weapons." *Autonomous Systems – Issues for Defence Policymakers*, 152-168. The Hague, Netherlands: NATO Communications and Information Agency, n.d.. https://www.act.nato.int/images/stories/media/capdev/capdev_02.pdf.

Rozin, Igor. "Russia to create first unit of battle robots by mid-2020s." Russia Beyond. 29 November 2019. https://www.rbth.com/science-and-tech/331349-russia-to-create-first-robots.

Sandner, Mark A.. "Future Unmanned Combat Air Vehicles (UCAV) and the Ethics of Responsibility." *Canadian Military Journal* 20, no. 1 (Winter 2019). http://www.journal.forces.gc.ca/Vol20/No1/page14-eng.asp.

Santoni de Sio, Filippo and Jeroen van den Hoven. "Meaningful Human Control over Autonomous Systems: A Philosophical Account." *Frontiers in Robotics and AI* 5, no. 15 (February 2018): 1-14. Last accessed 2 April 2020. https://www.frontiersin.org/articles/10.3389/frobt.2018.00015/full.

Scharre, Paul D. *Autonomous Weapons and Operational Risk*. Washington, D.C.: Center for a New American Security, 2016. Last accessed 4 April 2020. https://www.cnas.org/publications/reports/autonomous-weapons-and-operational-risk.

Scharre, Paul D. "The Opportunity and Challenge of Autonomous Systems." *Autonomous Systems – Issues for Defence Policymakers*, 3-26. The Hague, Netherlands: NATO Communications and Information Agency, n.d.. https://www.act.nato.int/images/stories/media/capdev/capdev_02.pdf.

Spiegeleire, Stephen De, Matthijs Maas and Tim Sweijs. *Artificial Intelligence and the Future of Defense – Strategic Implications for Small- and Medium-sized Force Providers*. The Hague, NE: The Hague Centre for Strategic Studies, 2017. https://hcss.nl/sites/default/files/files/reports/Artificial%20Intelligence%20and%20the%20Future%20of%20Defense.pdf.

The Russian Federation. *Examination of various dimensions of emerging technologies in the area of lethal autonomous weapons systems, in the context of the objectives and purposes of the Convention*. 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. 10 November 2017. https://www.unog.ch/80256EDD006B8954/(httpAssets)/2C67D752B299E6A7C1 2581D400661C98/$file/2017_GGEonLAWS_WP8_RussianFederation.pdf.

Turnbull, Charles (U.S. Mission to International Organizations in Geneva). Speech. U.S. Statement on LAWS: Potential Military Applications of Advanced Technology, First Session of the Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS), Geneva, 25 March 2019. https://geneva.usmission.gov/2019/03/26/u-s-statement-on-laws-potential-military-applications-of-advanced-technology/.

United Nations Institute for Disarmament Research. "Current Research - The Weaponization of Increasingly Autonomous Technologies (Phase III)." Last accessed 29 April 2020. https://www.unidir.org/projects/weaponization-increasingly-autonomous-technologies-phase-iii-2.

United Nations Institute for Disarmament Research. *Report of the 2019 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems*. Geneva: UNIDIR. 25 September 2019. https://www.unog.ch/80256EE600585943/(httpPages)/5535B644C2AE8F28C125 8433002BBF14?OpenDocument.

United Nations Institute for Disarmament Research. *The Weaponization of Increasingly Autonomous Technologies: Considering How Meaningful Human Control Might Move the Discussion Forward*. Geneva: UNIDIR. https://unidir.org/files/publications/pdfs/framing-discussions-on-the-weaponization-of-increasingly-autonomous-technologies-en-606.pdf.

United Nations News. "Autonomous Weapons That Kill Must be Banned, Insists UN Chief." 25 March 2019. https://news.un.org/en/story/2019/03/1035381.

United States. Congressional Research Service. *Defense Primer: U.S. Policy on Lethal Autonomous Weapon Systems*. Last modified 19 December 2019. https://fas.org/sgp/crs/natsec/IF11150.pdf.

Wolfgang, Meldon *et al*. "Gaining Robotics Advantage." Boston Consulting Group. 14 June 2017. https://www.bcg.com/publications/2017/strategy-technology-digital-gaining-robotics-advantage.aspx.