DEFINING THE EMERGING NOTION OF “MEANINGFUL HUMAN CONTROL” IN WEAPON SYSTEMS

THOMPSON CHENGETA*

The emerging notion of “Meaningful Human Control” (MHC) was suggested by the UK-based NGO Article 36 as a possible solution to the challenges that are posed by Autonomous Weapon Systems (AWS). Various states, NGOs, and scholars have welcomed the MHC proposition. Although other terms such as “appropriate levels of human judgment” have been suggested, MHC has gained more traction. The challenge remains, however, that both the terms MHC and “appropriate levels of human judgment” are not defined in international law and as of present, there is no literature that extensively or normatively defines either of the terms. From a normative standpoint, the choice between MHC and “appropriate levels of human judgment” is inconsequential since the definition that one ascribes to either of the terms will still be applicable to the other. To that end, this Article discusses questions that are helpful in defining MHC—and by extension “appropriate levels of human judgement”—and it concludes by proposing a working definition.

The control exercised by humans over weapons is changing in both nature and degree. Early weapons were mere tools in the hands of fighters who exercised direct control. With the advancement of technology, however, there has been considerable automation of the control that was previously exercised by humans. Moreover, the invention of drones introduced remote control to weapons systems, making it possible for humans to project force while thousands of miles away from the target. On the horizon are AWS—robotic weapons that, once activated, do not need any further human intervention. In the case of AWS, humans seem to be surrendering or delegating control of weapons to computers. While this may seem convenient, efficient, and safe for those deploying them, AWS raise far-reaching concerns. For that reason, many scholars and organisations are insisting that there is a need to maintain MHC over weapons—preferably, as a legal requirement. In order to define MHC, I propose that the international community must ask the following questions:

(1) What is the purpose of MHC? What is it that the international community is trying to resolve?

* Postdoctoral Fellow, South African Research Chair in international law, University of Johannesburg; Non-Resident Fellow, Institute for International and Comparative Law in Africa, University of Pretoria, Expert member, International Committee for Robots Arms Control (ICRAC); Panellist, International Panel on the Regulation of Autonomous Weapons, LLD., University of Pretoria, LL.M., Harvard, LL.M., University of Pretoria, LL.B., Midlands State University.
(2) Who should exercise MHC over weapons and when? Is the focus on manufacturers, programmers, the individuals who deploy weapons, or all of the above?

(3) Over what aspects of AWS should one exercise MHC?

In answering these questions, one of the major concerns that emerges about AWS is the potential that they may create a legal responsibility vacuum. For that reason, this Article argues that the nature of MHC exercised by humans over AWS must ensure that the weapon user is potentially responsible for all ensuing actions of the robots. To define the nature of control that allows responsibility, this Article considers the international law jurisprudence on the notion of “control” as the basis for responsibility. It argues that such control should be exercised over the “critical functions” of AWS, in particular, those that relate to decision-making. There are already disagreements in the AWS debate as far as what decision-making means. Accordingly, this Article discusses how that term should be defined as a step towards the definition of MHC.

There are various actors involved in the development and deployment of AWS. The fundamental question is whether the definition of MHC should focus on a particular actor or whether the term should be defined as a cumulative concept—summing up the different roles that are played by designers, roboticists, programmers, manufacturers, states and combatants. This Article argues that if MHC is meant to be a legal standard upon which the responsibility for use of AWS is determined, then one of the common mistakes among debaters is the attempt to define MHC without a specific actor in mind. The suggestion that the definition of MHC should be a standard focussing on a specific actor—in particular, fighters—is not to imply all other actors should be forgotten. Rather, the term MHC should zero in on the end users of the technology, producing a standard upon which the obligations of the other actors are couched.
I. INTRODUCTION

Autonomous Weapon Systems (AWS)—machines that, once activated, are able to make the decision to kill humans without further human intervention—pose serious legal, ethical, and moral challenges. While some scholars have argued that AWS have the potential to save lives on the battlefield, I have argued elsewhere that AWS cannot comply with interna-


tional humanitarian law and other international law standards that relate to the protection of the right to life and dignity.\textsuperscript{4}

Various solutions—amongst them a preemptive ban—have been proposed to solve the challenges posed by AWS.\textsuperscript{5} Article 36, a United Kingdom-based NGO, proposed and coined the idea of “Meaningful Human Control” (MHC) over weapon systems as a possible solution.\textsuperscript{6} This emerging notion that humans must maintain “meaningful control” over the

\begin{itemize}

\item \textsuperscript{5} At present, AWS do not exist and therefore have not been deployed, although they are at an advanced stage of development. In 2013, the UN Special Rapporteur on extrajudicial, summary or arbitrary executions, Christof Heyns, called for a worldwide moratorium on the production of AWS until the international community reaches a consensus. See generally Heyns, \textit{supra} note 2. Recently, in March 2016, Christof Heyns, in collaboration with another United Nations Special Rapporteur issued another report calling for a ban on AWS that do not have ‘meaningful human control.’ See Christof Heyns (Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions) & Maina Kiai (Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association), \textit{Joint Rep. on the Proper Management of Assemblies at the Thirty-First Session of the Human Rights Council}, ¶ 67, U.N. Doc. A/ HRC/31/66 (Feb. 4, 2016).

\end{itemize}
weapons they use has been supported by many commentators, states, and non-governmental organisations.\(^7\)

While MHC remains undefined by international law, it may serve as an important entry point towards finding a solution to the challenges posed by AWS.\(^8\) In three informal expert meetings of the Convention on Conventional Weapons (CCW) on Lethal Autonomous Weapon Systems (LAWS), many states and organisations emphasised the need to maintain MHC over weapons.\(^9\) During the fifth CCW Review Conference from December 12 to 16, 2016,\(^10\) states formalized the debate on AWS by establishing an open-ended Group of Governmental Experts (GGE) to meet for a period of ten days in 2017.\(^11\) The GGE will submit a report on its findings to the 2017 Meeting of the High Contracting Parties to the CCW. It is likely that in 2017 the GGE will discuss what MHC entails.

This Article proceeds in four parts. Part II provides a historical perspective on human control over weapons from an international humanitarian (IHL) and weapons law (IWL) standpoint. First, it will show that human control over weapons has been an important historic norm and is inherent in IHL.

---


\(^8\) Id.


and IWL. Second, it will discuss the factors considered to be responsible for the decreasing direct human control over weapons that is currently on-going. The use of armed drones is examined as an example of how the nature of human control over weapons has been changing from direct control to remote control. Part II also considers the serious moral and ethical issues raised by remote control of weapons. Drone technology is, in a way, where humanity has begun to draw a line in the sand regarding what forms of control are acceptable and unacceptable.

Part III emphasizes the importance of understanding machine autonomy, human autonomy, and control. To appreciate the challenges of AWS and in turn be able to define MHC in weapon systems, it is important to understand the difference and nuances of machine and human autonomy. This is followed by Part IV which discusses the origins of MHC and contributions of some scholars, organisations, and states to its conception. Thus, while MHC does not yet have a definition in international law, many scholars, states, and organisations perceive it as a potential solution to the challenges posed by AWS.

Part V seeks to propose a working definition of MHC by considering three questions: (1) the purpose of MHC, (2) who should exercise it and when, and (3) over what aspects of AWS should it be exercised over. Scholars continue to disagree as to what entails making the decision to kill and whether a machine or robot can make a decision to kill or if it is simply executing a pre-programmed human decision. Therefore, this Part will consider what decision-making means on the battlefield with particular reference to kill-decisions. It will also argue that the main purpose of MHC is to ensure responsibility over the use of weapon systems. Accordingly, it will discuss the jurisprudence on control in an attempt to formulate aspects of MHC. Finally, the Article concludes by proposing the following working definition of MHC:

MHC of weapon systems by a combatant or fighter [operator] is control of a nature that ensures the potential responsibility of the operator for all the resulting actions of weapon systems that he or she activates. Such control entails that:

(a) The decision to kill and the legal judgment pertaining to individual attacks must be made by a
human in real time, i.e. the actual time during which a target is to be killed.

(b) The weapon system depends on the authorization of the operator to execute his or her decision to kill.

(c) The weapon system has an abort mechanism that allows the operator to abort an attack in the event that it is no longer lawful to kill a target due to changed circumstances or other reasons prescribed in international law.

(d) Operators have an inherent obligation to monitor weapon systems they activate while the weapon systems execute operators' decision to kill.

II. HISTORY OF INTERNATIONAL HUMANITARIAN LAW'S TREATMENT OF HUMAN CONTROL OF WEAPONS

A sword never kills anybody; it is a tool in the killer’s hand.  

From time immemorial, weapons were understood to be mere tools in the hands of the fighter. Humans exercised “direct control” over weapons and were completely responsible over weapons they used. They were, in the strict sense, “masters” of their weapons. The traditional relationship between the weapon and the fighter is captured by retired U.S. Major General William H. Rupertus when he wrote about his rifle:

This is my rifle. There are many like it, but this one is mine. My rifle is my best friend. It is my life. I must master it as I must master my life. My rifle, without me, is useless. . . . I will learn its weaknesses, its strength, its parts, its accessories, its sights and its barrel. I will keep my rifle clean and ready. . . . We will


become part of each other. We will. Before God, I swear this creed. \(^{14}\)
The idea that weapons are mere tools in the hands of fighters and humans being the masters of such weapons has been echoed by the International Committee of the Red Cross (ICRC), \(^{15}\) which argues that the decision as to when to employ a weapon, against whom, and with what severity remain the preserve of fighters. \(^{16}\)

The concept of “direct control” of weapons by humans was also contained in the 1949 Geneva Conventions and their 1977 Additional Protocols, whose provisions invoke the idea that without human control or use, a weapon is nothing but a mere tool. For example, in armed conflict, participating in hostilities is shown by the “bearing of arms.” \(^{17}\) Thus, persons “who have laid down their arms” are considered to be “taking no active part in the hostilities.” \(^{18}\) Moreover, in non-international armed conflicts, one of the criteria for identifying organised armed groups is “that of carrying arms openly.” \(^{19}\) In international armed conflicts, classification as combatants is also determined by carrying arms openly. \(^{20}\)

These provisions all suggest that when an enemy combatant has “laid down his arms,” he or she is considered hors de combat—outside the fight. \(^{21}\) On the battlefield, an intention to surrender can also be shown by laying down one’s weapon. \(^{22}\) Consequently, it is only legitimate to harm enemy combatants when they still carry weapons. Thus, in the history of armed


\(^{15}\) HRW, *Shaking the Foundations*, supra note 4.

\(^{16}\) *Id.*


\(^{18}\) *Id.* art. 3(1) (common to the four Geneva Conventions).

\(^{19}\) *Id.* art. 13(2)(c); Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea art. 13(2)(c), Aug. 12, 1949, 75 U.N.T.S. 135.


\(^{22}\) *Id.*
conflict and development of weapons, a weapon was considered capable of doing harm only when it was in the hands of a human fighter. Even with the advent of armed drones, weapons are still in the hands of the fighter, albeit through remote control. But the advent of AWS means that direct control will soon no longer be a given feature of weapons.

The following section shows that, over the years, direct control over weapons has become untenable for various reasons. Accordingly, human control over certain aspects of weapons has been delegated to machines in a number of military contexts.

A. Factors Contributing to the Decrease in Human Control over Weapons

Three main factors have influenced the reduction of control exercised by humans over weapons: safety, convenience, and effectiveness. Delegating some degree of control to machines or computers is not only convenient but makes it safe for the user of the weapon while at the same time effectively achieving the military objective.

Ron Arkin, for example, has argued that the situation on the battlefield has become so precarious that it is unreasonable to expect humans to operate in such an environment.23 In the most traditional definition of “direct control” over weapons, however, a human being needed to be physically present to “pull the trigger.” This meant that the human fighters needed to physically avail themselves on the battlefield to make their weapons work. Thus, primitive explosive devices required the human fighter to hide somewhere nearby, sometimes waiting for days, until such time as the enemy combatant appeared for him or her to detonate the explosive by way of pulling a wire or trigger. Not only was this inconvenient and inefficient, but it also required the fighter to place his life at risk. Human control over many explosive devices was subsequently automated by allowing detonation of a weapon when certain pre-set parameters were met,24 such as anti-personnel landmines.25

25. While anti-personnel landmines are an early example of weapons automation, they were subsequently prohibited by international law.
Among other factors, success on the battlefield is largely determined by the speed at which one projects harm to the enemy and the extent at which one reduces risk to oneself. These factors have influenced the development of various military technologies that reduce the role that humans play on the battlefield in order to increase efficiency and reduce risk of harm. In fact, developments in weapons and the changing nature of war have made humans “the weakest link” on the battlefield. This is primarily driven by developments in military technologies that allow computers to process data in nanoseconds, allowing them to act significantly faster than humans. In this regard, the role of humans—especially the control they exercise over certain weapons—has been decreasing.

Although the reduction of control that is exercised over weapons by humans may be convenient, safe, and effective, it threatens some of the most important tenets of IHL and IWL. To emphasise this point, the following section considers how human control over weapons or use of force has been an important factor in the shaping of IWL.

B. Human Control over Weapons and the Rules of International Weapons Law (IWL)

There are three basic principles of IWL: the prohibition of weapons that cause superfluous harm and suffering, the prohibition of weapons that cause damage to the environment, and the prohibition of weapons that are indiscriminate in nature.

The proscription against weapons that are by nature indiscriminate, which is also a norm of customary international
law (CIL), is a cardinal principle of IWL. This rule is the basis for the restriction of use of weapons such as poison; antipersonnel landmines; cluster bombs; booby-traps; and incendiary, chemical, biological, and nuclear weapons. The rule is premised on the notion of human control over weapons they use. For a weapon to be legal, it must be capable of “being directed at combatants and military objectives” and must not have “effects that an attacker cannot control.” Accordingly, there are two elements that are part of the definition for indiscriminate attacks under customary international law that are consistently invoked when deciding whether a weapon is indiscriminate by nature: the capability of being directed against a specific military object and the capability to limit the effects of the weapon.

The first element of the CIL definition succinctly points to the notion of human control over weapons. It is the human who “directs” the weapon. It invokes the mechanistic control that humans must exercise over weapons they use. The second element of the indiscriminate rule points to the requirement of human control over the effects of the weapons they use. The requirement of human control over the effects of weapons they use is echoed in the military manuals and official reports of numerous states. Furthermore, many states have al-

---

art. 5(3) (as amended), May 3, 1996, 2048 U.N.T.S. 93, 133; Additional Protocol I, supra note 20, arts. 48, 51(4)(b), 51(4).

30. Henckaerts et al., supra note 21, at 1554–82 (discussing state practice for Rule 71).

31. Id.


33. Henckaerts et al., supra note 21, at 270–90 (discussing state practice for Rule 12, which defines “indiscriminate attacks”).

34. See, e.g., Additional Protocol I, supra note 20, art. 51(4)(b).

35. Id. art. 51(4)(c).

36. This in turn is a cornerstone in the establishment of the responsibility of weapon users. It could not and cannot be a defense for one to say it was not me, the weapon did it. Such scenarios would arise where machines or computers are in control of weapons and the results thereof are unpredictable to the persons activating the systems.

37. See Henckaerts et al., supra note 21, at 1505–81 (discussing state practice for Rules 70 and 71).
ready taken the position that a weapon should be deemed indiscriminate when a human cannot control its effects. 38

Anti-personnel land mines, one of earliest forms of automated weapons, have been nearly universally banned because they are non-discriminative in nature. 39 Once they are buried in the ground, the human fighter has no control over them. While the human fighter may have planted the landmine with the intent of targeting a specific person, once they are in the ground, the harm that will be caused by anti-personnel landmines becomes potentially unpredictable. The individual who placed the landmine can no longer control whom it will kill unless the landmine is strictly monitored. International condemnation towards the use of anti-personnel landmines is so strong that even the United States is now considering becoming a party to the treaty banning anti-personnel landmines. 40

The unpredictability of a weapon is one of the major concerns implicated by the advent of AWS. The history of human control over weapon systems and the rules of IWL demonstrate that the notion of human control over weapons has always been an important concept. Yet, the developments in military technologies, culminating with the creation of AWS, are slowly delegating the control over weapons from humans to computers.

C. Human Control over Weapons and Drone Technology

The concern over the manner and extent by which humans exercise control over weapons has been a frequent aspect of the debate on drone technology. Like other long range and projectile weapons, the development of drones was driven by the desire to project harm while being insusceptible to the same harm. Drone technology, however, introduced a new form of control over weapons—remote control. Despite this significant change, the control that is exercised over weapons in drone technology—albeit by remote control—has been largely ruled to be sufficient and acceptable, leading to the

38. Id.
39. See Ottawa Convention, supra note 25.
general agreement that drones are not illegal weapons per se.41

While drones have been largely accepted as legal, some commentators have separated the legal acceptance of drones from ethical arguments about the use of drones. In particular, some have objected to the use of drones because they allow the user to be physically removed from the battlefield.42 These critics argue that physical removal from the battlefield increases the likelihood that the drone “pilot” will be psychologically removed, leading to “trigger happy” behaviour.43 Thus, from an ethical point of view, the quality of control that a drone operator exercises over weapons may be affected by the mode he or she is using to control the weapon. Phillip Alston and Hina Shamsi suggest that this physical and psychological removal may have several consequences for drone warfare:

Equally discomforting is the PlayStation mentality that surrounds drone killings. Young military personnel raised on a diet of video games now kill real people remotely using joysticks. Far removed from the human consequences of their actions, how will this generation of fighters value the right to life? How will commanders and policy makers keep themselves immune from the deceptively antiseptic nature of drone killings? Will killing be a more attractive option than capture? Will the standards of intelligence gathering justify a killing slip? Will the number of acceptable collateral civilian deaths increase?44

Thus, while drones may not be illegal weapons per se,45 remote control of weapons produces troubling ethical questions.46 While the ethical concerns raised by drone technology

41. Heyns, supra note 2, ¶ 13.
42. Id. ¶ 14; see also Philip Alston & Hina Shamsi, A Killer Above the Law, Guardian (Feb. 8, 2010), http://www.guardian.co.uk/profile/philip-alston.
44. Glyn Williams, supra note 43.
45. Heyns, supra note 2, ¶ 13.
46. Other scholars have refuted these objections and argued that because drone operators are removed from the danger, it allows them to exercise better control over weapons than if they were on the “hot” battlefield
are serious, AWS raise an even more critical question—whether humans are still in control of the weapons they use.

Semi-autonomous weapon systems\textsuperscript{47} that are already in existence have changed the relationship between the weapon and the fighter from a “master-tool relationship” to one more similar to a partnership—albeit humans still exercising some level of control. Yet, the remaining control which humans still exercise over weapons is threatened by the advent of weapon systems with full autonomy—AWS.\textsuperscript{48}

Although weapon systems with full autonomy are not yet in existence, when they are finally deployed, they will be able to identify, search, track, and decide who to kill without human assistance or intervention once they are activated.\textsuperscript{49} Accordingly, various scholars, NGOs, and international organisations have expressed concerns over such kinds of weapons, indicating that without proper control by humans, these weapons may not be able to comply with the law—specifically, rules that protect the right to life and dignity.\textsuperscript{50}

III. UNDERSTANDING MACHINE AUTONOMY, HUMAN AUTONOMY, AND CONTROL

Three important points are fundamental to understanding the issues regarding human control and AWS. First, auton-
omy in weapon systems does not denote “free will” as it is understood in the philosophical discourse.\textsuperscript{51} In political philosophy, individual autonomy refers to “the capacity to be one’s own person, to live one’s life according to reasons and motives that are taken as one’s own and not the product of manipulative or distorting external forces.”\textsuperscript{52} Machines, however, cannot have this same type of human autonomy.

Second, autonomy can be incorporated into various functions of a weapon system, such as tracking, landing, taking off, and navigating—the non-critical functions. Autonomy in these non-critical functions does not create significant concerns, and in fact such autonomy is helpful. An increase of autonomy in non-critical functions of a weapon system means a decrease in the operator’s need to pilot the unmanned systems.\textsuperscript{53} In essence, autonomy in non-critical functions enables “the weapon system to be operated rather than continuously piloted.”\textsuperscript{54} When operators do not have to focus on non-critical functions such as navigation, it means their workload is decreased and they have more “time available for them to focus on decision-making”—which is the critical function.\textsuperscript{55} On the other hand, there are ethical and legal concerns on autonomy in the critical functions of weapon systems—those that relate to the selection of targets and the making of the decision to kill.\textsuperscript{56} Thus, while machine autonomy in the non-critical functions of a weapon system is desirable since it potentially increases the quality of human decision-making regarding choices humans make in relation to the life and wellbeing of other humans,

---


\textsuperscript{54} Id. at 12.

\textsuperscript{55} Id. at 60.

\textsuperscript{56} Id. at 3, 63.

\textsuperscript{57} Id. at 3, 63.
machine autonomy in critical functions is undesirable because it essentially removes human input in the making of an ultimate choice.

Third, autonomy in weapon systems exists on a spectrum.58 This spectrum can range from situations where the human thinks and assesses a target before enabling the weapon system to attack, a weapon system that provides a number of targets but leaves it to the human to choose which one to attack, a weapon system that selects targets from a pool and asks for a “go-ahead” from a human before attacking, a weapon system that selects the target and only give the human operator restricted time to override its choices, and a weapon system that selects targets and initiates the attack without human involvement.59 Paul Scharre has summarized the spectrum of autonomy as follows:

If the human is selecting the specific target or particular group of targets to be engaged, then the weapon is *semi-autonomous*. If the machine is selecting the specific targets and the human is observing in real-time and can intervene if necessary, then the human is exercising on the loop control over a *human supervised autonomous weapon*. And if the machine is selecting the specific targets and the human is unaware or unable to intervene, then the human is out of the loop for the selection of specific targets and the weapon is *fully autonomous*.60

Autonomy in weapon systems and human control are interrelated: the more the machine gains autonomy over the critical functions, the less control is exercised by humans. All decreases in human control may not be inherently bad; it is only when control is decreased to a certain point that the lack of control constitutes a violation of international law. The important question is at what point does the decrease in human control over weapon systems become unacceptable?


60. Scharre, supra note 58.
Machine autonomy in the execution of critical functions is not necessarily undesirable, because "computers are better and more efficient at performing some tasks than humans."

At the same time, humans are better at other tasks that machines are not good at, such as those that require human judgment or intuition. A total exclusion of either humans or computers will not be in the best interest of humans.

**Figure 1: The Relationship between Machine Autonomy and Human Control.**

Figure 1 shows how, for the critical functions of a weapon system, the more the system is allowed autonomy to execute critical functions without human input, the more human control (or rather, the meaningfulness of human control) is affected. While the relationship between machine autonomy and human control is not a zero-sum game, the more machine autonomy there is over the critical functions the less predictable the machine is, and the more the individual deploying it is left in the dark.

61. Sharkey, supra note 59, at 310.
Thus, because humans must exercise control over weapon systems, there must be a balance between human and machine effort.\(^\text{62}\) It is that balancing—not the exclusion of one or the other—that can “ensure precision and accurate targeting with less collateral damage and better predictable compliance with International Humanitarian Law.”\(^\text{63}\) But the same question still remains: at what point on the spectrum is the balance struck and at what point is it upset? The answer to this question is that humans must retain decision-making powers over the weapons they deploy. Therefore, the mere involvement of a human “in the loop” for the execution of critical functions does not necessarily mean that he or she is exercising meaningful control.

Almost all legal, moral, and ethical objections to AWS originate from the fact that AWS take humans “out of the loop” from the critical functions of weapon systems. Christof Heyns has noted that “taking humans out of the loop risks taking humanity out of the loop,”\(^\text{64}\) implying that where humans are out of the loop, there is no MHC. These concerns led to a number of questions. In what ways are humans taken out of the loop by AWS? Can it be argued that humans remain in the loop at all times by virtue of the fact that it is humans who preprogram the robots in the first place? Other scholars have asked whether, in AWS, humans are in the loop, on the loop, in the wider loop, or out of the loop.\(^\text{65}\) Leading roboticist Ron Arkin has highlighted “informal commentary where some individuals state that a human will always be in the loop regarding the application of lethal force to an identified target.”\(^\text{66}\) Similarly, the United States has long maintained the position that, notwithstanding advances in autonomous systems, humans will always remain in the loop.\(^\text{67}\) Thus, the critical question today is

\(^{62}\) Id.

\(^{63}\) Id.

\(^{64}\) Heyns, supra note 2, ¶ 89.

\(^{65}\) Id. ¶ 39.


\(^{67}\) See Peter Singer, In the Loop? Armed Robots and the Future of War, BROOKINGS (Jan. 28, 2009), http://www.brookings.edu/research/articles/2009/01/28-robots-singer. Some military commentators maintain that there
what is meant by “human in the loop” and whether it is the equivalent of MHC.

The terms human in the loop and consequently human out of the loop were first used by the U.S. military and in the computing fields after John Boyd put forward a theory on the human decision-making processes. According to Boyd, in making decisions, human beings “observe, orient, decide and act.” This has come to be known as the OODA loop, wherein a person observes his or her surroundings through his or her human senses, orients themselves to the information observed, and weighs possible reactions before deciding a course of action.

The think-act paradigm of machines and robots follows the OODA loop as they carry out information acquisition, analysis, decision selection, and action implementation. If

“will always be a need for the intrepid souls to fling their bodies across the sky” in armed conflict, and therefore humans will remain in the loop. Id.


72. Id.

faulty or incorrect information is taken in at the observe stage, it affects the rest of the loop. For that reason, human beings have remained in the loop for the purposes of monitoring and verifying decisions made by machines or robots. This has especially been the case where life or death decisions are involved.

The level of any robot’s or machine’s autonomy has thus been measured by the extent to which it is dependent on humans when performing the OODA loop. Where an unmanned system interacts with humans to complete the OODA loop, then humans are said to be in the loop; where it does not, humans are considered to be out of the loop. The determination of whether an unmanned system is autonomous or has a human being in the loop is based on three factors. First, the rate at which the machine requires a human in the loop to execute its “critical functions.” The more independent an unmanned system is once activated—determined by whether it requires further human intervention to operate—the more the machine is considered to be autonomous. Second, the ability or inability of an unmanned system to function successfully in an unstructured and unpredictable environment points to the machine’s level of autonomy. Where an unmanned system is able to adapt to an environment which was not predicted in the laboratory or at the time of activation, it is considered autonomous. Third, the level at which an unmanned system can assert its operational decisions when executing its functions also determines whether it is autonomous or automated. An unmanned system that has the capacity to exercise discretion in executing its task is more fully autonomous. Such an unmanned system may even independently alter how it completes a certain task while still achieving the same ends.

In addition to doubts that states will keep humans in the loop, while being in the loop may be a component of MHC,
it is not its equivalent. This is so because “to say that a human is in-the-loop does not clarify the degree of human involvement.”

Humans have psychological limitations—not only in certain environments, but also when they work alongside machines. Because humans are capable of deliberative reasoning, they can also be victims to errors of inductive reasoning, such as automation bias, assimilation bias, and confirmation bias.

Automation bias occurs when humans trust machine judgment to such an extent that they second guess themselves. Assimilation bias occurs when humans see what they want to see or hear what they want to hear. This is what the Nobelist Daniel Kahneman in his book *Thinking, Fast and Slow* has termed “WYSIATI”—“what you see is all there is.” A human drone operator, for example, while “seeking out patterns of behavior to determine a lethal drone strike, then seeing people load bales of hay or shovels onto a truck could initiate a causal story that they were loading rifles for an attack.”

Confirmation bias, also known as scenario fulfilment, occurs

loop: “[That] sounds more like brainwashing than actual analysis. Their mantra is a bit like the line they repeat again and again in the movie The Manchurian Candidate. Sergeant Shaw is the kindest, bravest, warmest most wonderful human being . . . . [Saying humans will always be in the loop] helps keep people calm that this isn’t the Terminators.” Singer, supra note 67.

79. Sharkey, supra note 59, at 310.


81. Sharkey, supra note 59, at 311.


83. DANIEL KAHNEMAN, THINKING, FAST AND SLOW (2011).


when humans, seeking to verify information, focus only on information that supports their already conceived beliefs.\(^{86}\)

In defining MHC, the temptation to equate it to the mere involvement of a human being in the loop must therefore be rejected. It is in this light that NGO Article 36 has observed that “having a person ‘in’, ‘on’ or ‘touching’ ‘the loop’ of a weapons system does not in itself ensure that MHC is exercised.”\(^{87}\) Instead, to ascertain what is meant by MHC, two normative questions must be asked. First, what is the purpose of MHC? And second, what should be the role of humans in the loop? Before answering these questions, it is necessary to consider the origins of MHC.

IV. The Origins of MHC in the AWS Debate

The UK-based NGO Article 36—whose mission is “to prevent the unintended, unnecessary or unacceptable harm caused by certain weapons”\(^{88}\)—was the first to coin the phrase “Meaningful Human Control” in relation to weapon systems.\(^{89}\) In doing so, Article 36 pointed out that the acceptability of a weapon or weapon system depends on the extent humans are in control of that particular weapon.\(^{90}\) At the 2014 United Nations Convention on Conventional Weapons (CCW) Expert Meeting on Lethal Autonomous Weapons Systems (LAWs)—the first CCW meeting on LAWs—Article 36 emphasised the need for “deliberative moral reasoning, by human beings, over individual attacks” and reiterated the call for a ban on weapons that do not allow MHC.\(^{91}\) To justify this requirement, Article 36 cited the IHL principle of humanity as the fountain


\(^{89}\) ARTICLE 36, supra note 87.

\(^{90}\) Id.

from which the notion of MHC flows, arguing that IHL requires “human commanders, the people upon whom the law bears, to make deliberative case by case judgements on the legality of individual attacks.”

NGO Article 36 also claimed that the requirement of MHC in weapon systems “is implicit in existing international law governing the use of force,” therefore making it ethically and legally unacceptable to develop or deploy weapons that are devoid of MHC. Accordingly, it asked member states to the CCW “to negotiate a new international legal instrument that would establish a positive obligation for MHC over individual attacks and by so doing prohibit weapon systems from operating without the necessary human control.” NGO Article 36 has reiterated the importance of MHC in its subsequent reports.

Other NGOs and international organisations have also supported or endorsed this emerging notion. In the context of law enforcement, Amnesty International voiced its concern that “weapon systems without MHC would not be able to correctly assess complex policing situations and comply with relevant standards, which prohibit the use of firearms except in defence against an imminent threat of death or serious injury.” Thus, Amnesty International argues that weapons without MHC are in many ways likely to violate important human rights, such as the right to life.

Human Rights Watch also sounded the same clarion notes during the 2014 CCW Meeting. It categorically stated that “there should always be MHC over targeting and kill deci-

---

92. Id.
93. Id.
94. Id.
97. Id.
sions”98 and observed that the key to a successful solution to AWS is “the emergence of a consensus that there should always be MHC of the targeting and kill decisions in any individual attack on other humans.”99 Furthermore, Human Rights Watch observed that determining the meaning and nature of MHC “is perfectly suited to CCW expert work.”100

In a report on its Expert Meeting on Autonomous Weapon Systems that was held from March 26-28, 2014, the International Committee of the Red Cross (ICRC) also reported that many participants in the meeting emphasised the importance of the notion of MHC over weapons systems.101 Furthermore, during 2014 CCW Meeting, the ICRC acknowledged that the notion of MHC was gaining traction and that, to understand the notion, there is a need to “examine current weapons that have autonomy in ‘critical functions’ to see how MHC is understood and considered to be implemented in practice today.”102 In a statement before the CCW Expert Meeting, the ICRC noted:

At some point on an incremental process of increasing autonomy in the “critical functions” of weapon systems, human control may no longer be meaningful. As we mentioned in our opening statement, we believe the crucial aspect is human control over the use of force, and what constitutes meaningful, appropriate and responsible human control over the “critical functions” of weapon systems. Where humans are so far removed in time and space from control over the weapon system, the human decision-making pro-

---

99. Id.
100. Id.
101. See generally Int’l Comm. of the Red Cross, supra note 53.
cess on the use of force may in effect be substituted with machine decision-making.\textsuperscript{103}

Aligning itself with other organizations, the Campaign to Stop Killer Robots indicated that “there is great concern with the prospect of future weapons that, once activated, would select and engage targets without MHC.”\textsuperscript{104} Accordingly, it has highlighted “the importance of always maintaining MHC over targeting and attack decisions.”\textsuperscript{105} Likewise, the International Committee for Robot Arms Control took note of the strengths and weaknesses of both machines and humans and concluded that it is only “the combined strengths of humans and computers operating together, with humans always in ‘meaningful control’ of targeting and engagement decisions [that] best serves military objectives and is the wisest path from a strategic, legal and ethical perspective.”\textsuperscript{106}

Numerous states have also referred to or supported the notion of MHC, indicating that it can possibly be the solution to the challenges posed by AWS. During the 2014 CCW meeting on AWS, a number of states expressed opinions supporting MHC. The German delegation issued a statement to the Chairperson that:

[W]e firmly believe that there should be a common understanding in the international community that it is indispensable to maintain “Meaningful Human Control” over the decisions to kill another human being. We cannot take humans out of the loop. We do believe that the principle of human control is already

\begin{flushright}


105. Id.

\end{flushright}
implicitly inherent in international humanitarian law which, I said before, remains a binding and guiding line also with regard to the new weapons systems. And we cannot see any more any reason why technological development should all of the sudden suspend the validity of the principle of human control.107

While acknowledging the newness and lack of definition of the notion, the German delegation observed that the notion of MHC is in fact "an indispensable principle of international humanitarian law."108 The view that MHC is a part of IHL was also supported by the delegation from Croatia.109

Switzerland also expressed strong sentiments regarding the issue of MHC. It noted that development and deployment of weapon systems that operate without MHC have far reaching ethical implications.110 The delegation from Switzerland thus highlighted that MHC could be the solution to the problem of AWS and delegates should strive to find what would constitute MHC.111

The Norwegian delegation contrasted weapon systems in existence with weapon systems with increased autonomy, noting that existing weapon systems have some form of MHC.112 In a statement that provided insight into a potential definition of MHC, Norway recalled that weapon systems already in the

108. Id.
111. Id.
employ of states are operated only in “tightly constrained spatial and temporal limits so that MHC is ensured.”

Although the United Kingdom did not acknowledge MHC during the 2014 CCW Meeting on Autonomous Weapon Systems, members of its government have. For instance, a parliamentary representative of the United Kingdom has already pointed out “that the operation of weapon systems will always be under human control.”

The delegation from the US also made some detailed comments on the emerging notion of MHC in its closing statement in the 2014 CCW Meeting:

There remains a lack of clarity regarding the concept of autonomous weapons decision making. As we have said, it is important to remind ourselves that machines do not make decisions; rather, they receive inputs and match those against human programmed parameters. . . . We have heard some discussion . . . about the relationship between human and machine. There have been many references this week to the notion of “Meaningful Human Control.” But from our perspective, this formulation does not sufficiently capture the full range of human activity that takes place in weapons systems development, acquisition, fielding and use; including a commander’s or an operator’s judgment to employ a particular weapon to achieve a particular effect on a particular battlefield. Crucially we also need to consider whether, through effective training of personnel, autonomous features of weapons system may be made more predictable; for instance, ensuring that [Autonomous Weapon Systems are] only used as intended and with full knowledge of [their] functioning could enhance precision and thus reduce collateral damage and risks to non-combatants.

113. Id.
Overall, MHC was one of the themes that consistently ran through the 2014 CCW Meeting and others that followed. The Chairman of the 2014 Meeting stated in his final report that:

Many interventions stressed that the notion of “Meaningful Human Control” could be useful to address the question of autonomy. Other delegations also stated that this notion requires further study in the context of the CCW.\footnote{See U.N. Office for Disarmament Affairs, Chairperson’s Rep. on the 2014 Informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWs) ¶ 20, http://www.unog.ch/80256EDD006B8954/%28httpAssets%29/350D9ABED1AFA515C1257CF30047A8C7/$file/Report_AdvancedVersion_10June.pdf (advanced version).}

A number of scholars have also referred to the notion of MHC. In his presentation at the 2014 CCW Meeting, roboticist Noel Sharkey emphatically stated that the international community “must maintain MHC in weapon systems.”\footnote{Sharkey, supra note 13.} The role of the human in the loop has been and must remain a legal principle;\footnote{Sharkey, supra note 59, at 319–21.} its erosion must be resisted and the international community must “lock down human supervisory control as a legal principle of human control.”\footnote{Id.} Sharkey argues that because of the inadequacy of current technology to make distinctions between military and civilian objects “we must ensure that the decision to kill remains firmly under human control.”\footnote{Sharkey, supra note 59, at 305.}

As a precautionary measure to counter any problems resulting from autonomy—problems such as “malfunctions, communications degradation, software coding errors, [and] enemy cyber-attacks”—Sharkey suggests that humans have to exercise MHC over weapon systems.\footnote{Id.}

Roboticist Ron Arkin has also acknowledged the use of the term MHC, noting that “there remains a long way to go even in terms of shared definitions and terminology regarding autonomy and MHC.”\footnote{Jefferson Morley, Autonomous Weapons Stir Geneva Debate, ARMS CONTROL ASSOC., (June 2, 2014), https://www.armscontrol.org/act/2014_06/news/Autonomous-Weapons-Stir-Geneva-Debate.}

\begin{thebibliography}{9}
\bibitem{}Sharkey, supra note 13.
\bibitem{}Sharkey, supra note 59, at 319–21.
\bibitem{}Id.
\bibitem{}Sharkey, supra note 59, at 305.
\bibitem{}Id.
\end{thebibliography}
Christof Heyns argues that the first step towards defining MHC “would be to take a collective decision now, before such weapons are deployed, that humans, whether in the narrow or wider loop, should retain meaningful control over each decision to launch a potentially deadly attack—and to ensure that this line is not crossed.” In calling for a definition of MHC, he points to the urgent “need to develop a clearer picture of what ‘meaningful’ or ‘appropriate levels of’ human control would entail.” Heyns observed that the notion of MHC “provides a popular standard to be used to distinguish acceptable from unacceptable uses of increasingly autonomous systems” that is worth of study.

Paul Scharre has observed that militaries are likely to prefer MHC over weapon systems:

All things being equal, militaries are likely to favour weapons that have greater connectivity with human controllers for sensible operational reasons. Keeping humans in the loop decreases the chances of weapons striking the wrong target, resulting in fratricide or civilian casualties, or that they simply miss their target entirely, wasting scarce and expensive munitions.

Mark Hagerott rightly observes that MHC is more applicable to weapon systems and asks an important question: “Where does ‘Meaningful Human Control’ fade away?” Some commentators have maintained the call for a pre-emptive ban of AWS because of a lack of MHC. They argue that a ban “is necessary to ensure the retention of ‘Meaningful Human Control’ over targeting and attack decisions, which in turn is necessary

125. Id. at 13.
126. Scharre, supra note 58.
to ensure that we uphold the principles of humanity as much as possible in the face of the already existing horrors of war and conflict."\textsuperscript{128}

Finally, Peter Asaro has noted that if the notion of MHC does not exist in international law as yet, there is need to establish it.\textsuperscript{129} It is evident, therefore, that the term MHC is gaining traction, quickly becoming a common term among scholars. Without a doubt, having common terminology is essential. However, that common terminology does not take the discussion any further as long as there are irreconcilable views on the basic moral and philosophical underpinnings that underlie the debate over MHC. Because there remain, for example, diverging views on whether robots should be given the power to make killing decisions and what decision-making means, it is predictable that debaters will not agree on what the term MHC entails.\textsuperscript{130}

V. DEFINING MHC IN WEAPONS SYSTEMS

There is no doubt that MHC can potentially provide some solutions to the problems posed by AWS. However, this will only be possible if MHC is correctly defined. The dictionary meaning of the word “meaningful” points to what is “significant, relevant, important, consequential, material, telling, pithy, weighty, valid, worthwhile, and purposeful.”\textsuperscript{131} The word “control” refers to “the power to influence or direct . . . behaviour or the course of events” through “charge, management, direction, guidance, supervision, superintendence, oversight influence.”\textsuperscript{132}

Accordingly, the literal meaning of MHC over weapon systems is the significant, material, or purposeful exercise of


\textsuperscript{130} See Asaro, supra note 4, at 696.

\textsuperscript{131} \textit{Meaningful}, \textit{OXFORD ENGLISH DICTIONARY}, http://www.oxforddictionaries.com/definition/english/meaningful.

\textsuperscript{132} Id.
power over machines to influence or direct their behaviour by controlling, directing, or supervising their actions. From this literal definition of MHC, I pose the following questions:

1. What is the purpose of MHC? What is it that the international community is trying to resolve?
2. Who should exercise MHC over weapons and when? Is the focus on manufacturers, programmers, the individuals who deploy the weapons, or all of the above?
3. Over what aspects of AWS should one exercise MHC?

A. MHC for What Purpose?

If the purpose of MHC is to address major challenges posed by AWS, identifying those challenges is critical to defining MHC. Although there is an array of challenges posed by AWS, the three chief concerns are that if AWS are given the power to make the decision to kill without human involvement, this may: (1) violate the right to life both in war and peace,133 (2) violate the right to dignity,134 and (3) lead to an accountability vacuum for such violations.135 The need to answer these questions has been echoed by Peter Asaro, who argues that in seeking to define MHC, “we should focus on the threats posed to fundamental norms of responsibility and accountability, and to the threats to human rights and human dignity that these new technologies present.”136

There is no doubt that human soldiers may equally threaten the right to life and violate the right to dignity, as can

---

133. HRW, Shaking the Foundations, supra note 4.
134. Id.
136. Asaro, supra note 1, at 386.
be seen in current armed conflicts.\textsuperscript{137} But when traditional weapons are used, humans can be held accountable for their actions. AWS, on the other hand, creates an accountability gap because humans are removed from the critical functions of the weapons system. This presents the greatest challenge for the adoption of AWS. Therefore, while MHC may not prevent violations of the right to life and dignity—as it can still be violated by humans themselves\textsuperscript{138}—it will help ensure that they are held accountable for their actions.

Accountability is key to ensuring the rule of law—there should always be some hands to cuff whenever a crime is committed.\textsuperscript{139} When there is a significant chance that the fighter will not be held accountable for the “actions of the machine” he deployed, then, he or she is not exercising MHC. Therefore, a machine should not be an independent actor; every action should be initiated by a human fighter so that he or she is responsible for the act.

MHC over weapon systems is necessary to ensure that there is no accountability gap. Other areas of international law address similar accountability gaps. For instance, both the law on state responsibility and international criminal law state that the nature of control that is exercised by state or actor “X” over “Y” determines whether “X” is responsible for the actions of “Y.”\textsuperscript{140} Similarly, the purpose of MHC is to ensure that where AWS are used, there is potential to hold someone responsible for resulting infractions.\textsuperscript{141}

\begin{itemize}
\item[138. Id.]
\item[139. See Walzer, supra note 135, at 287.]
\item[140. See Mark Bovens et al., The Oxford Handbook of Public Accountability 214 (2014); Eric Marsden, Control and Accountability in Highly Automated Systems 4 (2011); Mohamed Othman, Accountability for International Humanitarian Law Violations: The case of Rwanda and East Timor 250 (2005).]
\end{itemize}
B. MHC by Whom, over What and When?

If MHC is meant to be a legal standard upon which the responsibility for use of AWS is determined, then MHC cannot be defined without a specific actor in mind. During the 2014 CCW meeting, the U.S. delegation argued against a formulation of MHC that “does not sufficiently capture the full range of human activity that takes place in weapons systems development, acquisition, fielding, and use.”\(^{142}\) There is a “range of human activity” from different actors, such as states, roboticists, designers, programmers, and manufacturers, that contributes to how AWS are ultimately controlled by the end users—the combatants. Such actors can determine or influence the nature and extent of control that is exercisable by the end users. The same is also true for simpler weapons such as guns. Yet the responsibility of a gun user is almost never conflated with that of a gun manufacturer. When gun manufacturers put in place safety measures like trigger locks, they are exercising some form of control. When a gun user unlocks that trigger lock and decides when to discharge the firearm and against whom, he or she is exercising ultimate control of the weapon. The difference in liability between the manufacturer and end-user may reflect that these actors exercise control at different times, in different ways, and in different circumstances.

When AWS are used and something goes wrong, however, responsibility is potentially established through different modes of responsibility that relate to different actors.\(^{143}\) Responsibility or accountability is important in international law because where there is an accountability gap, the victims’ right to a legal remedy is adversely affected.\(^{144}\) There are generally four modes of responsibility: individual, command, corporate, and state responsibility.\(^{145}\) Under individual and corporate re-

\(^{143}\) See Docherty, supra note 141.
sponsibility, there is civil and criminal liability. I have discussed in detail the challenges of AWS to these modes of responsibility elsewhere.\textsuperscript{146}

In short, however, these modes of responsibility are complementary to each other; they are not alternatives to the exclusion of the other.\textsuperscript{147} For example, if AWS create an accountability gap—as far as the individual criminal responsibility of those deploying AWS on the battlefield is concerned—that specific gap is neither closed by suing the responsible individuals under civil responsibility nor holding the manufacturing company liable under corporate responsibility for example.\textsuperscript{148} More importantly, in terms of international weapons law, there cannot be “split-responsibility” over use of a weapon—where responsibility is divided or shared between the fighter and other persons involved in the production of AWS like manufacturers.\textsuperscript{149} Legally, each actor is responsible in their independent capacity. For example, individuals involved in the production of AWS have their own responsibilities for their participation in the designing, manufacturing, selling, and transferring stages.\textsuperscript{150}

In all this, state responsibility is like an umbrella to all the forms of responsibility mentioned above: covering and enforcing corporate responsibility at the design stage of AWS up to selling or transferring stage, enforcing individual and command responsibility when the weapon is finally used on the battlefield or law enforcement situations.\textsuperscript{151} As one commentator has observed, when considering accountability over the ac-


\textsuperscript{148} Bianchi, supra note 147, at 17; Steinhardt, supra note 145, at 531–32.

\textsuperscript{149} Steinhardt, supra note 145, at 531.

\textsuperscript{150} Int’l Comm. of the Red Cross, supra note 53, at 8.

\textsuperscript{151} Id. at 89–90.
tions of AWS, state responsibility "is the frame of reference for considering other forms of international responsibility." 152

For the above reasons, if MHC is to be a legal standard upon which responsibility is established, it cannot be defined without specifying for which actors the term is being defined. Specifying the actor is essential to creating a workable legal standard. Thus, in addition to asking the question over what aspects of AWS should humans exercise meaningful control, there is a need to ask a specific and targeted question as to who is exercising MHC. This suggestion that the definition of MHC should be a standard focussing on a specific actor is not to imply that all other actors should be ignored.

While it is generally agreed among commentators that AWS may result in an accountability gap, the actor whose liability is affected and in what way is often unidentified. Thus, discussions of the accountability gap or the responsibility of actors, suffer from the following three flaws which may lead to a faulty definition of MHC:

(1) States, corporations, and individuals are lumped together, suggesting that a summation of the different roles they play—from production to fielding of AWS—may constitute MHC. In this sense, MHC is a wide and cumulative concept embracing a wide range of human activity that goes into production and fielding of AWS. 153

(2) As a result of the above, responsibility for actions of AWS is split or shared among the various actors that are involved in the production and deployment of AWS. 154


Consequently, the accountability gap problem does not exist and if it does, it is solved if one of the actors can be held accountable.\textsuperscript{155}

Conceptualizing MHC in such a generalized or broad sense is only correct when pointing to the contribution of a range of actors who are involved in the development and fielding of AWS. But when defining MHC as a legal standard—at least one that is workable and in line with existing international standards for responsibility—then, there is a need to narrow down the definition to a specific actor.

I suggest that the definition of MHC should focus on the end users of the technology—the fighters or combatants. In this regard, a “focused” question should be asked: What does MHC of weapon systems by a fighter or combatant mean? There are three main reasons I choose to focus on what is meant by MHC of weapon systems by fighters or combatants: First, the problem of the accountability gap posed by AWS as discussed by scholars largely affects the responsibility of fighters or combatants—the final users of the technology. If AWS are unpredictable, it is difficult if not impossible to ascertain the mens rea of the person deploying them, thereby obfuscating the establishment of individual criminal responsibility.

Second, when determining the responsibility of a weapon-user for a war crime committed, the focus is on the bearer of the weapon not its manufacturer for example.\textsuperscript{156} This is because it is the combatant or fighter who is in control of a weapon and who makes choices regarding which weapon to use. This does not mean, however, that a manufacturer cannot be a co-perpetrator, aider or abettor of the crime if certain

damental principle that no penalty may be inflicted on a person for an act for which he or she is not responsible”).


conditions are fulfilled—including being a party to the armed conflict.\textsuperscript{157} But generally, companies and their workers are not party to an armed conflict unless they directly participate in an armed conflict.\textsuperscript{158}

Third and final, when formulating the definition of MHC of weapon systems by a fighter or combatant, the role and obligations of other actors will inevitably be created. Thus, the definition of MHC of weapon systems by a fighter or combatant creates a standard upon which the obligations of other actors, especially those who are involved in the production or development of AWS, can be formulated.

When defining MHC of weapon systems by fighters or combatants, individual criminal responsibility should be adopted as the relevant standard of responsibility. For there to be MHC, the control exercised over weapon systems by a combatant should be of such a nature that the actions of a weapon system are the intended outcome of the combatant deploying it. This does not mean combatants who use weapon systems in a negligent manner are not held responsible. Such negligent combatants are still subject to IHL rules that govern those who use their weapons without regard to whether civilians or protected persons are affected.\textsuperscript{159} In short, the definition of MHC should ensure that all weapon systems—like traditional weapons—remain tools in the hands of fighters.\textsuperscript{160}

C. Individual Criminal Responsibility of Combatants and Control over Weapon Systems

The responsibility of fighters or combatants over war crimes or other violations of international law is established through individual criminal responsibility and command re-

\textsuperscript{157} Timothy McCormack \& Avril McDonald, Yearbook of International Humanitarian Law 84 (2006).
\textsuperscript{158} Id.
\textsuperscript{159} See, e.g., Hector Olásolo, The Criminal Responsibility of Senior Political and Military Leaders as Principals to International Crimes 101 (2009).
sponsibility.\textsuperscript{161} Under individual criminal responsibility, the nature of control exercised by a fighter over a weapon has never been at issue because, from time immemorial, weapons have been mere tools in the hands of fighters.\textsuperscript{162} Even while there have been moral and ethical objections to the nature of control exercised over armed drones, legally, the remote control of drones is acceptable because such drones still remain tools in the hands of their operators.

Individual criminal responsibility holds a combatant criminally liable in their personal capacity.\textsuperscript{163} A combatant’s criminal responsibility is a result of their direct contribution to the crime, either by participating, ordering, planning, instigating, inciting, co-perpetrating, engaging in a joint criminal enterprise, or aiding and abetting.\textsuperscript{164}

Individual criminal responsibility requires both an \textit{actus reus} and \textit{mens rea}.\textsuperscript{165} Yet in the case of AWS, it is the robot that is physically on the battlefield carrying out the relevant acts after reaching its own decision. Thus, the issue is whether the actions of the robot are in fact the outcome of the fighter’s intentions, and can therefore be attributed to the human actor. Furthermore, where there is no human intervention once the robot is activated and the robot is operating in an unstructured environment, its actions may be unpredictable. This will make it difficult—if not impossible—“to distinguish when a system is under control, [or] when an operator has lost control”\textsuperscript{166} and to determine the \textit{mens rea} of the combatant.\textsuperscript{167}

A fundamental question when AWS are used is who is making the decision to kill or use force? A key concern on the use of AWS is that life and death decisions must not be made by machines.\textsuperscript{168} Thus, MHC of weapon systems by a combatant should require the human combatant to exercise decision-


\textsuperscript{162} Docherty, supra note 141.

\textsuperscript{163} See Sildregt, supra note 161.

\textsuperscript{164} Id.

\textsuperscript{165} Id.

\textsuperscript{166} Asaro, supra note 1, at 385.

\textsuperscript{167} Docherty, supra note 141, at 19–20.

\textsuperscript{168} Asaro, supra note 4, at 687–709.
making power. The question then becomes how one can define “decision-making” in the context of AWS targeting.

D. Defining Decision-Making as an Element of MHC in Weapon Systems

There are already disagreements as to what “decision-making” means in relation to AWS targeting. For example, during the 2014 CCW Expert Meeting, the U.S. delegate noted:

There remains a lack of clarity regarding the concept of autonomous weapons decision-making. As we have said, it is important to remind ourselves that machines do not make decisions; rather, they receive inputs and match those against human programmed parameters . . . .169

That approach, however, is a limited portrayal of the decision-making processes on the battlefield. In the context of armed conflict, the decision to kill occurs in at least two parts. First, the decision to kill or to use force is made by humans when they program or set parameters that warrant targeting. Second, the robot analyses situations on the battlefield, comparing it to the set parameters—the box-ticking process. The second part of this decision-making process is fundamental. In real time, a flawed analysis by the robot may lead to an incorrect decision to release force. This is exacerbated in unstructured environments and where AWS may act in an unpredictable manner.170

This two-step decision-making process is comparable to a human commander who deploys his human soldiers. The human commander gives a specific command, for example, he orders his human subordinates to kill the enemy combatants. Human soldiers’ understanding of who is the enemy combatant is defined by certain parameters and IHL rules. They are supposed to kill only those who are directly participating in hostilities. When human soldiers arrive on the battlefield, they will only release force against those who fit the pre-defined parameters.

of who is an enemy combatant. While the combatants are
given the order to kill and whom to kill before leaving the mili-
tary base, the real decision-making on the actual release of
force is made on the battlefield. Similarly, Peter Asaro has
noted that the “rules of engagement are not decisions to en-

gage or use force—rather they are guidance to human deci-
sion makers who will [finally] make those decisions and carry
the responsibility for them.”

It is the analysis of facts on the battlefield and fitting them
to pre-defined parameters that constitute the real decision-
making to kill. Accordingly, when human combatants recuse
themselves—and machines instead carry out the analysis—
then they cannot claim to be the ones making the decision to
kill. The situation on the battlefield is so unpredictable that if
weapon systems are given autonomy in analysing whether a sit-
uation meets the set parameters and making legal judgments,
then, for all intents and purposes, it is the robot that is making
the decision to kill. Combat is a “highly complex and almost
chaotic system” requiring “decision-making to be robust
against rogue outcomes.” The nature of the battlefield
shows that preprogramed determinations or parameters alone
cannot suffice as decision-making; the battlefield requires
human “mental and physical flexibility to be able to react as
the outcome [of battlefield events] unfolds.” In order to
have a “clear communication of intent from commanders to
subordinates throughout the chain of command,” there
should be “strong interactions between forces.” Above all,
IHL “imposes specific requirements on the decision makers,
who are implicitly human.” The mere fact that one has set
the parameters within which AWS are supposed to operate on
the battlefield does not make their eventual choices the deci-
sions of humans.

“combat is fundamentally a human phenomenon” that is “dominated by
human behavior,” thus focusing on the importance of human input in real
time on the battlefield).
172. Asaro, supra note 1, at 378.
173. Storck, supra note 171, at 130.
174. Id.
175. Id. at 131.
176. Asaro, supra note 1, at 378.
177. Id.
Of course, the question that has characterised the AWS debate is: what if robots can make better decisions than humans? This seems a compelling argument, especially in circumstances where it appears the better decisions of AWS may save lives. Marchant et al, relying on Arkin’s earlier work, refer to a number of reasons why robots may be able to make better decisions than human combatants. AWS are created without emotions; they do not act out of anger, frustration, revenge fear, or hysteria which in the battlefield always influences human combatants to “press . . . toward fearful measures.” Moreover, because AWS are non-human and lack the need for self-preservation, they can act conservatively. For example, an AWS may be designed to only use lethal force only when they are fired upon, improving decision-making. If AWS are in fact capable of making better decisions than humans, Jonathan Herbach has argued that there would be an obligation to use them.

The question, however, is not only about who can make a better decision between humans and robots but who should make the decision. Arguably, there can be circumstances where children can make better decisions than adults, yet because of IHL rules on child soldiers, children cannot legally participate in armed conflict. The prohibition is out of the need to protect children and also because they cannot be prosecuted for any infractions of the law. Thus, decision making to use force is subject not only to legal constraints, but also to moral and ethical ones. Only the kill decisions that are made by humans are acceptable because only humans are capable of

181. Marchant et al., supra note 179, at 280.
morality and ethics.\textsuperscript{185} For the purposes of respecting the right to dignity of both the persons deploying AWS and those who are targeted, it is important that humans retain the power to make the decision to kill.\textsuperscript{186} As Peter Asaro argues, every killing of a human being must be meaningful:

For the killing of a human to be meaningful, it must be intentional. That is, it must be done for reason and purpose. Philosophically, intentionality requires understanding the meaning and significance of an act. . . . In the absence of intentional meaningful decision to use violence, the resulting deaths are arbitrary and their significance along with the dignity of those killed is dismissed.\textsuperscript{187}

AWS can neither understand the implications of their actions nor can they wield an intention. Neither a machine nor its algorithm can make a legal or moral judgment for which it can take responsibility. Decision-making is the litmus for determining who is in control and control is the basis for responsibility in international law. For that reason, for a combatant to be in MHC of a weapon system, the combatant must be responsible for making the decision to kill or release force against human targets in real time.

Michael Schmitt, however, has argued that “the mere fact that a human might not be in control of a particular engagement does not mean that no human is responsible for the actions of the autonomous weapon system.”\textsuperscript{188} He argues that because the robot is programmed by a human, there is always a human to hold responsible for any resulting war crimes.\textsuperscript{189} This approach is not correct because it treats the various modes of responsibility in international law as if they were alternatives.\textsuperscript{190} A combatant’s responsibility for using a particular weapon is not absolved by the fact that a programmer or manufacturer of that weapon can also be held responsible.

Schmitt also ignores the problem of unpredictability of AWS that is created by high levels of autonomy and function-

\textsuperscript{185} Asaro, supra note 1, at 385.  
\textsuperscript{186} Id.  
\textsuperscript{187} Id.  
\textsuperscript{188} See Schmitt, supra note 32, at 33.  
\textsuperscript{189} Id.  
\textsuperscript{190} Supra Section B.
ing in unstructured environments. If followed to its logical conclusion, Schmitt’s argument is that once an AWS has been programmed and deployed, all the eventual actions of the AWS are attributable to the programmer or the individual deploying it. In this regard, Schmitt’s argument suggests that programming of an AWS alone is sufficient control by the weapon user leading to responsibility for all ensuing acts. There can be situations where a combatant with no intentions to commit any crime deploys an AWS to kill legitimate targets but the system—because it has decision-making powers exercisable without the intervention of a human—makes an unlawful choice. Thus, where AWS have the power to make important decisions without human intervention, such decisions may not be in line with the intentions of the person deploying them. This is why I have emphasised the need for humans to participate in real time when the decision to kill is made.191

A human should be in control of the system for each individual attack because such control is central to establishing the responsibility of combatants. For there to be meaningful control, programming alone is not sufficient. In order to fulfill the responsibility requirements of international law, the human combatant must be able to approve targets and prevent or abort missions whenever the situation requires—exercising MHC control in real time.

E. Using Jurisprudence on Control to Define MHC in Weapon Systems

Control as an element of establishing responsibility is a familiar concept in international law.192 It has been discussed and given meaning in various branches of international law such as international human rights law, IHL, ICL193 and the

191. Supra Section D.
192. See Amy Tan, Responsibility and Control in International Law and Beyond, THE HAGUE INSTITUTE FOR GLOBAL JUSTICE (June 27, 2013), http://www.thehagueinstituteforglobaljustice.org/latest-insights/latest-insights/news-brief/responsibility-and-control-in-international-law-and-beyond/ (noting that experts have found an increase in courts and tribunals utilizing the notion of effective control).
193. Id.
constitutive elements of a public body in international trade law.194

In 2013, a group of international law experts gathered to discuss the notion of “control” in international law as a mode of responsibility and how it impacts other fields.195 One of the experts, Kristen Boon, indicated that the ICL notion of “command responsibility”—in particular the element of “effective control”—has an impact in other branches of law such as the law of occupation, the law of state responsibility, and international human rights law.196 During the meeting, it was noted that the notion of “effective control” is often applied “differently in different contexts,” but with the “the basic compulsion behind the legal inquiry being the same: who is the aggregator of power, who can be held accountable, and which facts are required to satisfy those tests?”197 As a starting point, fighters or combatants who use AWS must be the wielders of power when critical decisions are made.

Some aspects of control that have been fleshed out by international courts can be useful in the current debate. For example, when discussing the notion of control to ascertain the responsibility of a state in cases concerning the Bosnian genocide and the United States’ support of paramilitary operations in Nicaragua,198 the International Court of Justice (ICJ) noted that under the strict control test and the effective control test, the level of control exercised by the state is determined by the


195. Dr. Kristen Boon (Seton Hall University), Dr. Carsten Stahn (University of Leiden) and Dr. Dov Jacobs (University of Leiden) made presentations at a discussion forming part of The Hague Institute for Global Justice’s Supranational Criminal Law Lecture Series on June 26, 2013. Tan, supra note 192.

196. See Id.

197. Id. (emphasis added).

level of dependence of a non-state entity on the state. The “dependence factor” developed by the ICJ can be helpful in formulating the elements of what is meant by MHC over weapon systems by fighters or combatants. Accordingly, MHC should include the dependence of weapon systems on a human fighters’ input to execute the “critical functions”—those functions in weapon systems that relate to selecting the target and making the decision to kill.

Under the “strict control” test, for a state to be responsible for the actions of a non-state entity, the relationship between the two parties must be “one of dependence on the one side and control on the other.” In the Paramilitary Activities case, the ICJ explained that dependence must be in all the important activities of the non-state entity to the extent that the non-state entity is “merely an instrument” or “agent” of the state. Control and dependence were thus held to be absent in circumstances where the non-state entity has a choice to pick from available options to the extent of differing from the supporting state.

In line with the “dependence factor” discussed above, MHC over weapon systems can be present when the relationship between fighters and AWS is “one of dependence on the one side and control on the other” for executing the critical functions of the weapons system. In executing the critical functions, the power to “choose” from available human targets

---


200. Int’l Comm. of the Red Cross, supra note 53.


must be exercised by the human fighter. Accordingly, AWS must be incapable of executing its critical functions without human assistance.

Adopting the language of these control tests, AWS should act “on the instructions of,” and be “under control” of humans in executing the critical functions of the weapons system if humans are to be held responsible. In each case of targeting, there must be a human being who is involved in the planning and choosing of targets. The human must be responsible for giving “specific directives and instructions” in the execution of the critical functions. To this end, preprogrammed instructions and “unspecified acts of involvement” in the execution of critical functions will not suffice as MHC of weapon systems by a fighter or combatant. For a state to be responsible for the actions of a non-state actor, it must exercise undeniable and decisive influence over an armed group whose survival is dependent on the aid of that state. The same relationship should exist between AWS and combatants deploying them. Humans must not be mere “approval mechanisms” for AWS but should actively participate and be decisively influential in the system’s targeting, having made the decision to use lethal force.

F. Relevance of Command Responsibility in Defining MHC

In the AWS debate and in particular in relation to the concept of MHC, some commentators have suggested that command responsibility can be used to establish the responsi-

207. Contrary to Michael Schmitt’s suggestion, discussed in supra Section D, AWS should not be allowed to complete a targeting mission without human involvement.
211. Asaro, supra note 1, at 385.
bility of those who deploy AWS. It is not uncommon that in the debate on AWS, some commentators refer to persons deploying AWS as the commanders while the AWS are referred to as agents. This gives an impression that AWS are replacing the human fighters as robot combatants.

Command responsibility—a concept founded and developed to govern the relationship between a human commander and a human subordinate—cannot be used to govern this new relationship between a human commander and a robot. Individuals who deploy AWS should not be labelled as commanders and AWS should not be labelled as agents or combatants. Whether this is done intentionally or unwittingly, referring to individuals who deploy AWS as commanders gives the impression that AWS are the combatants or fighters, hence the temptation to wrongly invoke the command responsibility mode. AWS must not be referred to or treated as combatants or fighters. They must be considered as weapons and when they are developed, they must not be given autonomy or functions that would transform them from weapons to “machine combatants.” The concept of command responsibility cannot and should not be applied to AWS—at least in the manner that has been suggested by some commentators. While the “effective control” element of command responsibility may be useful in fleshing out MHC, that is different from using command responsibility to define liability for the use of AWS.

In ICL and IHL, command responsibility as a mode of computing criminal liability has been introduced and developed as a concept governing the relationship between a human commander and a human subordinate. Referring to the person who deploys AWS as a commander is wrong and misleading. Even the literal meaning of “commander” states that it is an individual in authority over a body of troops during a military

214. Rome Statute, supra note 29, art. 28.
operation.\(^{215}\) In IHL and ICL, a commander has been understood to be a natural person exercising authority over natural persons in a military operation.\(^{216}\) Likewise, Article 28 of the Rome Statute uses terms such as “forces” and “subordinates” who are capable of being subjected to prosecution and punishment.\(^{217}\) Because machines cannot be subject to criminal prosecution, it is evident that the drafters of the Rome Statute intended, and rightly so, for the concept of command responsibility to be applied only to human to human relationships.

Moreover, a consideration of the key elements of command responsibility shows that it is a concept developed strictly to govern the relationship between humans on the battlefield. In order for a commander to be held responsible for the actions of his or her subordinate, there are three important elements that must be satisfied:

1. That the commander knew or ought to have known that crimes were about to or were being committed by his or her subordinates;
2. That the responsible commander failed to prevent or stop commission of the crimes by his or her subordinates;
3. And that the commander did not punish the subordinates after the fact.\(^{218}\)

The above elements have been consistently applied by courts to establish command responsibility.\(^{219}\) The first two elements refer to commanders and subordinates, terms that have consistently been used to refer to humans, not machines. More importantly, the third element refers to the duty of the commander to punish his or her subordinates when they commit crimes. Machines have no moral agency and cannot be

---

217. Rome Statute, supra note 29, art. 28.
218. Id.; Additional Protocol I, supra note 29, arts. 86(2), 87.
punished.\textsuperscript{220} Thus, the concept of command responsibility was and still is meant to apply to only human to human relationships on the battlefield. And while concepts of law are sometimes extended to cover and address new situations, this cannot and should not be done for command responsibility and AWS, as have been discussed above.\textsuperscript{221}

Thus, in regard to the concept of command responsibility and AWS, Peter Asaro also observes that:

> The nature of command responsibility does not allow one to abdicate one’s moral and legal obligations to determine that the use of force is appropriate in a given situation. One might transfer this obligation to another responsible human agent, but one then has a duty to oversee the conduct of that subordinate agent. Insofar as autonomous weapon systems are not responsible human agents, one cannot delegate this authority to them.\textsuperscript{222}

The same reasoning that applies to traditional weapons carries over to AWS. Command responsibility is only relevant to AWS when the commander or civilian who supervises the combatant deploying an AWS knew or should have known that his or her subordinate was using an AWS in an unlawful manner and did nothing to prevent or stop his or her subordinate or punish them after the fact.\textsuperscript{223} AWS are weapons and those who deploy them are the warriors. From a legal perspective, AWS cannot and should not commit crimes. As Seneca observed, “a sword is never a killer, it is a tool in the killer’s hands.”\textsuperscript{224} Therefore, if this is a case of a warrior and his weapon, to establish liability of the combatant or fighter over the use of weapon systems, the correct mode of imputing criminal liability is individual criminal responsibility.\textsuperscript{225}


\textsuperscript{221} See Docherty, \textit{supra} note 141, at 19–26.

\textsuperscript{222} Asaro, \textit{supra} note 4, at 701.

\textsuperscript{223} See Schmitt, \textit{supra} note 32, at 33.

\textsuperscript{224} \textit{Id.} at 1.

\textsuperscript{225} Marco Sassoli, \textit{Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified}, 90 INT’L L. STUD. 308, 324 (2014). Although Sassoli uses the term “commander” to refer to the individual deploying the AWS, he also states that “it is obvious
There are, however, certain elements of control that have been developed under command responsibility that can be useful in fleshing out the definition of MHC over weapon systems by a combatant—specifically the notion of “effective control.” In order to be held accountable for the actions of his or her subordinates, the commander must have exercised effective control over them. Determination of responsibility is a question of “effective exercise of power or control and not of formal titles.”

Effective control that a commander ought to exercise must be, in the strict sense of the word, “effective.” It should not be merely theoretical or potential. The International Criminal Court has found that a “substantial influence over subordinates” alone does not meet the threshold of effective control over subordinates. Similarly, MHC over weapon systems by a human fighter must be real, not “theoretical or potential.”

that a commander deploying autonomous weapons must understand how they function, just as for any other means and method of warfare. In my view, the responsibility of such a commander is not a case of—nor is it analogous to—command responsibility, but a case of direct responsibility, just as that of a soldier firing a mortar believing that it can land only on the targeted tank, but which will kill civilians he knows are following the tank. This is a question of the mens rea, intent and recklessness with which criminal lawyers are familiar.”

---


230. See Milos et al., Case No. X-KR-05/24-3, Verdict at Second Instance, at 37.

Humans must not only remain in the loop but actively participate in that loop.

In summary, in defining or constructing MHC as a legal standard, the following must be emphasised:

1. The major purpose of MHC is to deal with the accountability gap challenge that is posed by AWS by holding those who deploy AWS responsible.
2. MHC should be narrowly defined. But there is need to define MHC with a specific actor in mind—the fighters or combatants. The definition of MHC of weapon systems by combatants or fighters should be determined in the context of individual responsibility.
3. The relationship between weapon systems and combatants must be one of control and dependence. Weapon systems must depend on human operators to execute critical decisions.
4. Human combatants should retain the decision making powers for executing critical functions. Decision making cannot be automated or preprogrammed; humans must participate in decision making in real time.
5. The actions of weapon systems must be the creation of the fighter or combatant deploying them.

G. Other Relevant Factors for MHC of AWS by Combatants or Fighters

In addition to these key points, there are a number of additional factors that highlight or inform whether a human combatant or fighter meets the MHC standard.

1. The Ability of a Combatant or Fighter to Observe and Act in Real Time

In order to meet the standard for MHC, the human combatant must not only actively participate in the analysis of the target and the making of legal judgements, but must also be able to—in real time—“perceive and react to any change or unanticipated situations that may have arisen since planning

the attack.”232 While set parameters may help a machine to analyse situations and make certain decisions, the battlefield is subject to unexpected twists and turns. Therefore, a human being must be able to exercise control in real time in order to respond to changing dynamics. For this reason, the International Committee for Robot Arms Control has observed that human operators should “have full contextual and situational awareness of the target area” and be “able to perceive and react to any change or unanticipated situations that may have arisen since planning the attack.”233

2. The Human Controller’s Active Participation in the Reasoning Behind the Attack

Pre-programing the parameters that AWS will use to make decisions is not sufficient to constitute MHC. Instead, the human controller must actively participate in the analysis of the target or “ticking of the boxes,” from the reasoning behind the attack to the point where force is released. In other words, merely being ‘in the loop’ is not sufficient to establish MHC.234

3. Sufficient Time for Deliberation on the Legality of the Target

A common concern generated by active human participation in the machine deliberation process is time. Now that machines or computers process data in nano-seconds,235 how can a human, who has become the “weakest link” on the battlefield,236 actively participate in the deliberation and analysis of a target or situation?

Despite these concerns, human beings must participate in the decision-making process. Thus, MHC should require sufficient time for the human operator’s “deliberation on the nature of the target, its significance in terms of the necessity and appropriateness of attack, and likely incidental and possible accidental effects of the attack.”237 This should be required even if it means slowing down the processing of the machine.

---

233. Sauer, supra note 106.
235. Heyns, supra note 2, ¶ 41.
236. Id. ¶ 53.
After all, like Noel Sharkey says, “there should be no hurry for humans to kill each other.”  

This view is supported by the International Committee for Robot Arms Control. It noted that for there to be MHC over weapon systems, “there must be active cognitive participation in the attack [by a human being] and sufficient time for deliberation on the nature of the target.” Similarly, Article 36 has argued that all legal judgments regarding the status of each particular target must be made by a human.

4. **Time Frame and Space Limitation on Operation**

It has also been suggested that MHC should be defined in terms of the time frame and space over which the AWS is used. The greater time and space that a particular system covers, the more it is likely that a combatant or fighter has no MHC over it.

NGO Article 36 notes that while most existing weapon systems can operate autonomously once they are activated, the “critical aspects of how human control is exercised over such weapons pertain to the programming of the target parameters and sensor mechanisms, and to the area within which and the time during which the weapon operates independently of human control.”

Thus, NGO Article 36 concludes that, inasmuch as human control over existing weapon systems is exercised through legal, policy, and technical limitations, the “size and geographical location of the target area and the time window are important determinants of human control exercised over weapon systems.”

The idea of space and time limitations has some merit. However, it also poses a number of challenges. First, the issue is not the amount of space or time over which the system can operate without human control; it is how much a machine can do and should be allowed to do without human control. A mere second without human control at the time or location...
that human control is needed may be more disastrous than
years without human control where it is unneeded.

Another example is that of an AWS that is capable of
searching for an individual on the basis of facial recognition. It
may not matter for how long the machine searches for the
individual for the purposes of targeting if the combatant who
deployed it is aware that the individual being sought is still a
legitimate target. Such awareness is achieved through constant
monitoring of the weapon system and the verification of the
status of the targeted person. In an armed conflict, if someone
continues to actively take part in hostilities, that individual is a
legitimate target. Therefore, to comply with IHL, it does not
matter how long the machine stays in combat searching for
that particular individual—as long as he or she continues to
directly participate in hostilities. Similarly, the size of space
that an AWS is programmed to search is irrelevant to the rules
of IHL; it is the nature of the area that matters. For instance,
an AWS deployed in a desert to search for terrorists may face
less difficulty compared to the one that is deployed in a high
density suburb. Therefore, issues of time frame and space cov-
ered are of limited help in calibrating the elements of what is
meant by MHC to meet the standard proposed above.

Second, defining MHC in terms of time and space limita-
tions may vitiate the already existing weapon systems that have
been accepted as consistent with international law, such as the
Israeli Harpy. The Israeli Harpy is a lethal Unmanned Ae-
rial Vehicle that is ‘designed to detect, attack and destroy ra-
dar emitters’ with a capability to scout a wide area for many
hours. But the fact that the weapon is already in existence
or that there have been no protests about it does not necessa-
rily mean that it has MHC. While the ability of the Israeli
Harpy to search a wide area for hours may not be an issue for
establishing MHC, its capacity to search for “targets not neces-
sarily known to the individual who launched it but those that
meet the Harpy’s programmed parameters” raises concerns

243. See “The Israeli Harpy”, ISRAEL WEAPONS, http://www.israeli-weap-
244. Id.; see also Paul Scharre, Autonomy, “Killer Robots” and Human Control
ty.org/12708/autonomy-killer-robots-human-control-force-part/.
245. Id.
because the decision to kill must be made by a human in real time. I have already indicated that the important part of decision-making is the assessment of facts in real time against set parameters.246 Furthermore, in the case of the Harpy, there may be no issues because it is not being used to make decisions to target humans, but rather as a defensive system.

5. The Availability of “Abort” Mechanisms

Another factor that has been suggested as a constituent of MHC is the existence of “means for suspension or abortion of an attack.”247 This has been suggested and supported by NGOs like the International Committee for Robot Arms Control.248 Some commentators, however, argue against this element, noting that some weapons that are already in existence, such as homing munitions “fire and forget,” have no abort mechanisms. Once the decision to launch them has been made, it cannot be recalled.249 For that reason, incorporating abort mechanisms into the definition of MHC may mean that various weapon systems that are otherwise legal would now be on the wrong side of the law.250

Similarly, some scholars thus observe that “some of the notions put forward for minimum necessary standards for meaningful control assume a level of human control far greater than exists with present-day weapons.”251 Paul Scharre argues that the discussion of MHC therefore “occurs in a vacuum, divorced from an understanding of how weapons actually exist today.”252 He concludes that a strict interpretation of the proposed standards so far will result in the banning of “virtually every weapon since the invention of the catapult.”253

These arguments are not entirely correct. Abort mechanisms are linked to the issue of when the decision to kill is actually made and by whom. What commentators have referred to as abort mechanisms do not occur after the final decision to kill has been made and force has been released.

246. Supra Section D.
248. Sauer, supra note 106.
249. Scharre, supra note 244.
250. Id.
251. Id.
252. Id.
253. Id.
There is no legal requirement to call back a bullet that has left the barrel.

An attack is a process. This includes the time when a human deliberates and assesses the legality of a target. If during that assessment—even at the very last minute—it appears to the human controller that something is not right; he should not proceed with the release of force. An “abort mechanism” can refer to two points in time. First, when a fighter’s finger is still on the trigger, if something changes, he can choose not to fire. Second, a fighter may make an assessment and conclude that certain targets are legitimate. Upon starting the release of force, he or she may recognise that the targets are not legitimate or are no longer legitimate and the fighter will stop firing.

After an assessment of the legitimacy of targets with the active participation of a human who then agrees to the release of force, if it appears that the targets are in fact not legitimate or no longer legitimate, there must exist a mechanism in all weapon systems that allow the fighter to stop or abort the firing. This does not refer to, as the critics seem to interpret it, the recalling of bullets already fired. Instead, it is about the ability to stop those still in the barrel from being fired. Such a requirement does not endanger existing weapon systems; it merely ensures that abort mechanisms that have always existed in weapons system will continue to be required.

H. Proposed MHC Definition

From the foregoing discussion, I propose the following definition for MHC:

MHC of weapon systems by a combatant or fighter [operator] is control of a nature that ensures the potential responsibility of the operator for all the resulting actions of weapon systems that he or she activates. Such control entails that:

(a) The decision to kill and the legal judgment pertaining to individual attacks must be made by a human in real time, i.e. the actual time during which a target is to be killed.

(b) The weapon system depends on the authorization of the operator to execute his or her decision to kill without which, it cannot proceed.
(c) The weapon system has an abort mechanism that allows the operator to abort an attack in the event that it is no longer lawful to kill a target due to changed circumstances or other reasons prescribed in international law.

(d) Operators have an inherent obligation to monitor weapon systems they activate while the weapon systems execute operators’ decisions to kill.

In the above sense, maintaining MHC over weapon systems means retaining the control-dependent relationship between humans and weapon systems for their critical functions. By adopting this definition of MHC, it can be ensured that weapon systems are predictable and their actions will, at all times, reflect the intentions of their operators. In essence, a properly constituted definition of MHC does not allow machines to be given full autonomy in executing the critical functions—those that involve the decision to kill. In other words, a properly and normatively construed definition of MHC is the equivalent to a ban on fully autonomous weapons.

Of course, the above proposed definition of MHC focusses on the fighter or combatant—the end user of the technology. The obligations of designers, roboticists, programmers, manufacturers and states as far as AWS are concerned should subsequently be couched in the above definition. For example, individuals and companies should be liable for designing, programming and manufacturing robots that can operate without the constraints proposed in the above definition. In turn, there should be a treaty or a Protocol to the CCW that spells out the obligations of states not to allow the designing, manufacturing, stockpiling and purchase of AWS that do not have constraints spelt out in the above definition.

VI. Conclusion

When defining MHC, there is a need to be clear as to what purpose it is meant to serve and over what aspects of AWS should one exercise meaningful control. More importantly, if MHC is meant to be a legal standard upon which the responsibility for use of AWS is determined, then the definition should be “targeted” or focused on a specific actor. Defining MHC of AWS in relation to combatants or fighters allows the rule devel-
oped to guide other actors on their responsibilities during production or development of AWS.

The major purpose of MHC is to deal with the accountability gap challenge posed by AWS relating to the responsibility of persons deploying the weapons. This purpose drives this Article’s proposed definition, which ensures that the relationship between weapon systems and combatants or fighters must be one of control and dependence. Although weapon systems can be allowed some form of autonomy, they must depend always on human operators to execute critical functions such as making the decision to kill. Thus, as indicated in the proposed definition, one of the critical factors essential to establishing a relationship of control and dependence between weapon systems and combatants is that humans should retain the decision-making powers for executing the critical functions of weapon systems. Decision-making cannot be automated or preprogrammed; humans must participate in decision-making in real time. Accordingly, the actions of weapon systems must be the brainchild of the fighter or combatant deploying them.