ORF ISSUE BRIEF
DECEMBER 2016
ISSUE NO. 165

Towards Policy Clarity on Autonomous Weapons Systems

JEREMY B. ENGLAND

ABSTRACT There is deep discomfort with the idea of a weapons system that surrenders life-and-death decisions to machines. The International Committee of the Red Cross (ICRC), an independent humanitarian organisation set up in 1863, has been playing an active part in discussions around the subject of Autonomous Weapons Systems (AWS). It argues that such debates should focus on determining the type and degree of human control required to ensure that in the use of AWS, there is ethical acceptability and compliance with International Humanitarian Law (IHL). Policymakers must consider variables like predictability, control of escalation, command responsibility, and legal accountability. Technological evolution will only continue to accelerate, impacting the way war is waged, and the imperatives are clear: The international community should make sure that AWS do not endanger more civilian lives. Stakeholders in Asia need to weigh in on this debate, and raise the questions explored in this paper.

INTRODUCTION

In today's interconnected world, marked by violence of all sorts, what would it take for you to feel comfortable standing in front of an autonomous weapons system (or AWS)? And how would you go about negotiating with one?

This is the acid test for making policies on which, one day, millions of people may have to rely for their safety. That day could come sooner than anyone expects. India's Permanent Representative in Geneva has said: "We cannot ignore the inexorable march of technology, in particular that of dual use nature, expanding the autonomous dimension of lethal weapon systems."[1] ORF scholar, Arun Mohan Sukumar meanwhile has written, "No Asian country has declared either its cyber capabilities or doctrines to manage cyber and cyber-physical[2] weapons."[3] There is a lot of work ahead for the international

community of policymakers, advisers and experts on autonomous weapons.

The very idea of a weapons system that places the use of force beyond human control, causes deep discomfort. For the International Committee of the Red Cross (ICRC), discussions should focus on determining the type and degree of human control required to ensure compliance with International Humanitarian Law (IHL) and ethical acceptability.[4]

AWS DEFINED

There is no existing internationally agreed definition of Autonomous Weapons Systems (AWS). Most accepted definitions, however, include the notion of a weapons system that can independently select and attack targets–a criteria that the ICRC agrees with. After initial activation by a human operator, the system itself–using sensors, computer programming and weapons–takes on the targeting process without human intervention. This distinguishes AWS from, for instance, armed drones—whose critical functions are still controlled by a human operator, albeit remotely. Based on this definition, such autonomy is no longer a futuristic concept reserved for sci-fi literature. It exists: and it is already being deployed today, primarily in defensive functions against objects such as air or missile defence systems and vehicle "active protection systems", but also in offensive roles such as certain missiles and loitering[5] munitions. AWS rely on information sensors and sources, on their built-in programming and on physical weapons and capacities. All three of these systems can be manipulated through cyber-attacks of various sorts.

A caveat is in order: The author of this article is not a technical expert, but a humanitarian-affairs one. This essay focuses on AWS, rather than wider cyber security, and will identify the questions that must be asked to develop effective and balanced policy on such new weapons. As professionals in humanitarian work, ICRC staff have spent plenty of time researching and convening debates on AWS and their potential effects. ICRC has a direct stake in the issues at hand, whether at the level of policy and law, or on the ground, where the humanitarian consequences of such weapons will ultimately be experienced and, consequently, responses will be required.

ICRC: A BACKGROUNDER

The International Committee of the Red Cross (ICRC), established in 1863, is a neutral, independent humanitarian organisation, directed by its international mandate to protect and assist victims of armed conflicts, and to promote implementation of, and respect for, International Humanitarian Law (IHL). Throughout its long history, the ICRC has spent substantial time dealing with different weapons and their effects–from laser blinding weapons to anti-personnel mines and cluster munitions, all the way through to Chemical, Biological, Radiological and Nuclear (CBRN) weapons. As far back as World War I, the ICRC called on States to prohibit the use of poisonous and asphyxiating gases, contributing to the adoption of the Geneva Gas Protocol in 1925. In each case, the ICRC is driven by facts of a weapons' use, not only the intentions of its design. The Committee supports States to strengthen or develop laws necessary to set appropriate limits or guidance on weapon use—based on first-hand observations of their human costs.

The ICRC also trains its staff on managing the risks associated with different weapons and how to develop meaningful responses for civilian populations who may be impacted by them. It encourages States to negotiate and adopt bans for anti-personal mines and cluster munitions, works to have unexploded ordnances cleared, helps people to understand and avoid the risks, or to recover and rehabilitate from their injuries or losses. In 2011, the ICRC assisted colleagues in Japan to manage the radiological hazards following the Fukushima incident. It currently trains hospital staff to cope

with patients potentially exposed to chemical contamination in Northern Iraq. But for certain weapons, such as nuclear, the ICRC knows that no institution (civilian or military) has adequate responses and technology to respond meaningfully to affected people's needs. This is one of the reasons the ICRC is calling upon States to ban the use of such weapons.

The chief concern with AWS, and the wider cyber security debate, is that there exists little practical experience of the effects of some of the new weapons under discussion, as well as how the international community might have to respond to humanitarian needs emanating from their use. At the same time, there is a great urgency to achieve clear guidance and frameworks. No one can be comfortable with further deployment of such weapons before the international community even manages to acquire a clear grasp of how to do so in a responsible manner. But how to know?

CURRENT FRAMEWORK AROUND AWS

The fundamental framework, which in the absence of more specific ones, covers AWS is International Humanitarian Law (IHL) and applies during armed conflict. It aims to mitigate suffering by protecting those who do not, or no longer, participate in the hostilities, as well as by regulating the conduct of hostilities. A fundamental principle of IHL is that the parties to an armed conflict do not have an unlimited choice of means and methods of warfare. All weapons, means and methods of warfare must be capable of being used – and actually be used – in accordance with IHL. In particular, they must comply with the rules aimed at protecting civilians from direct or indiscriminate attacks (and as far as possible from any other effects of the hostilities), and with the rules protecting combatants from unnecessary suffering. The key question is whether it is possible to use an AWS in a way that respects rules of distinction, proportionality and precautions in attack.

Fortunately, there is consensus that evolving technologies of war must comply with IHL. All weapons require assessment and legal review under Art. 36 of Additional Protocol 1 before they are developed or acquired. However, all States have an interest in assessing the legality of new weapons in order to ensure that their armed forces can conduct hostilities in accordance with international legal obligations, the principles of humanity, and the dictates of public conscience. The important question with any new technology review is not whether it is 'good' or 'bad' in itself, but to consider the particular characteristics of the weapon, the circumstances of its use, and its compatibility with IHL.

Views on AWS continue to evolve, including those of the ICRC. But discussions amongst States, experts and civil society indicate broad agreement that some 'meaningful', 'appropriate' or 'effective' human control over weapon systems and the use of force must be retained. More discussion is required on the kind and degree of control needed to make it 'meaningful' from a legal, ethical and operational perspective. These questions are difficult but the notion of human control is the overarching issue in AWS debates.

'MEANINGFUL HUMAN CONTROL': DEFINITION AND IMPERATIVE

Is it technically possible to programme AWS to carry out complex, context-dependent assessments required by IHL, wherever they encounter protected persons or objects? Or are these inherently qualitative assessments that require uniquely human reasoning and judgement? A clear majority of States worry about this; a group of experts said in 2014: "There is serious doubt that autonomous weapons can ever be programmed in a way to guarantee [...] compliance with relevant international laws."[6] Even if such weapons are made compatible with IHL, the question is if

people are prepared to surrender to machines the task of making life-and-death decisions.

Answering these questions would give some guidance to the kind and degree of human control required for AWS. Four domains of enquiry help further clarify the parameters of 'meaningful human control':

- The ability to control a weapon and the use of force is linked to its predictability and reliability. If AWS are programmed to adapt and learn, they are inherently unpredictable–the system itself has control on how it functions and human control is lessened. A degree of predictability is also lost when autonomous weapons carry out more complex tasks or are deployed in more dynamic environments. So, what level of predictability and reliability is considered necessary?

- How will the resort to the use of force, possibly triggering an automatic escalation of the use of force, be controlled in the case of AWS whether employed in an offensive or defensive capacity? Could autonomous weapons trigger or rapidly escalate conflict, making it harder for political decision-making and control—for instance along militarised borders where strategic restraint is what helps to hold back all-out war? How and when would human intervention in the functioning of the weapon work to assure oversight of its activation, supervision during its operations, and ability to deactivate should the situation change?

- How does one identify the command structures responsible for AWS? Identification in cyber-attacks is difficult enough–how will AWS be identified and to whom can civilians, or humanitarian organisations like the Red Cross, intervene with if and when AWS operate in a way that does not comply with IHL?

- Finally, and most importantly, how will the accountability in cases of violations of IHL be enforced? It is the parties to the conflict that are responsible for respecting, and ensuring respect for, the rules on the conduct of hostilities. These obligations cannot be transferred to a machine. Negligence in programming or deployment of such machines remains a human responsibility. The programmers, commanders and ultimately States (or non-State actors) must be accountable for violations of IHL. Who wants the responsibility for the actions of an AWS if they have no means to control it?

This last point appears crucial in helping to legally define what constitutes meaningful control.

A NEW LEGAL INSTRUMENT FOR AWS?

Discussions leading to Inter-State agreements often begin with definitions–but there is no clear definition of 'autonomous weapon systems' and that may prove to be a distraction. There are existing international legal principles and it can already be seen that some weapons are autonomous in their critical functions of targeting and attack. This existing and emerging technology must be viewed to assess the level of human control necessary under existing IHL rules and principles to help determine where the limits on autonomy should be placed.

The ICRC advocates for a positive obligation for human control over weapons and the use of force. Future international discussions will need to determine the kind and degree of human control necessary to ensure compliance with IHL and ethical acceptability. Agreement on such control could, in due course, lead to additional legal developments to ensure that all new weapons systems, and those that deploy them, adhere to those limits.

LOOKING AHEAD

The ICRC continues to engage with numerous States and other actors on the above challenges, including at the meetings of experts of the Convention on Certain Conventional Weapons (CCW) in Geneva over the past three years. It has also convened two of its own international expert meetings[7] in March 2014 and March 2016 (both in Geneva) with the participation of 21 States. States now need to take the CCW discussions to the next stage, developing greater technical and legal clarity and better understanding of the requirements for human control under IHL. This should ultimately inform agreement on where the limits on autonomy should be placed and decisions as to whether more specific laws should be developed. The ICRC will need the engagement of all key stakeholders in these processes.

The questions raised in this brief are relevant to all States, not just those developing the new technologies of warfare. All stakeholders need to weigh in on the debate. Equally important is that Asian thinkers and Asian States must help define what weapons can be deployed and what limits on autonomy should be enforced–unless they wish to fall victim to the decisions of others. The policy advice that the international community should be working on is one that gives an assurance that, in times of conflict, each person will be clearly distinguished in relation to legitimate military targets, that there will be ways to intervene to control unintended consequences or escalation resulting from AWS use, as well as clear means to hold those deploying AWS accountable as and when needed. Second, the international community must make sure that such weapons, while putting less military lives at risk, do not put more civilian lives at risk in the process. Sadly, it is an indisputable trend that over the last 100 years, modern warfare and weaponry has only increased civilian deaths. The burden of proof lies with each new generation of weapons.

Technology will continue to evolve at an ever accelerating pace, impacting weapons and thus the way war is waged. International deliberations around the legality of lethal autonomous weapons (LAWS) is unlikely to decrease the rate of their development.[8] The international community will need to move fast to keep up with them–the questions raised are not ones which can be left for future generations to resolve. They must be addressed now, with responsibility and urgency, to ensure that advances in weaponry do not outpace our capacity to protect ourselves. ORF

The key elements of this essay were first shared by the author at the ORF CyFy Conference Panel dedicated to ***Sentient Technologies, Cyber Weapons and Autonomous Platforms****, held in New Delhi on September 29, 2016. For additional ICRC resources, refer: https://www.icrc.org/en/war-and-law/law-and-policy)*

ABOUT THE AUTHOR

Jeremy B England is the Head of the International Committee of the Red Cross (ICRC) Regional Delegation (covering Bhutan, India, the Maldives and Nepal).

ENDNOTES:

1. Statement by PR to CD at the CCW Informal Meeting of Experts on Lethal Autonomous Weapons Systems, April 11, 2016.
2. Cyber-physical weapons are partly or fully automated platforms.
3. ORF Special Report (July 2016). *The Case for Cyber and Cyber-Physical Weapons: India's Grand Strategy and Diplomatic Goals*, Arun Mohan Sukumar.
4. Statement of the ICRC, read at the Meeting of Experts on Lethal Autonomous Weapons Systems, Convention on Certain Conventional Weapons, Geneva, 11-16 April, 2016. https://www.icrc.org/en/document/statement-icrc-lethal-autonomous-weapons-systems?language=en.
5. Loitering munitions are weapons systems that are deployed into a wide geographic area for a long period of time and can carry out strikes autonomously.
6. Statement from Austria in the 2014 Meeting of Experts on LAWS.
7. Expert Meeting Report (2016). Expert Meeting Report (2016). *Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons*, Geneva, ICRC, https://www.icrc.org/en/publication/4283-autonomous-weapons-systems.

   Expert Meeting Report (2014). *Autonomous weapon systems technical, military, legal and humanitarian aspects*, Geneva, ICRC. https://www.icrc.org/en/document/report-icrc-meeting-autonomous-weapon-systems-26-28-march-2014.
8. Bedavyasa Mohanty, Command and Control: India's Place in the Lethal Autonomous Weapons Regime, ORF Issue Brief May 2016, Issue No. 143.

OBSERVER RESEARCH FOUNDATION
Ideas • Forums • Leadership • Impact

20, Rouse Avenue Institutional Area, New Delhi - 110 002, INDIA
Ph. : +91-11-43520020, 30220020. Fax : +91-11-43520003, 23210773
E-mail: contactus@orfonline.org
Website: www.orfonline.org