AUTONOMOUS WEAPON SYSTEMS UNDER INTERNATIONAL LAW

BY

BERKANT AKKUS

A THESIS SUBMITTED TO ABERYSTWYTH UNIVERSITY FOR THE DEGREE OF DOCTOR OF PHILOSOPHY IN THE DEPARTMENT OF LAW AND CRIMINOLOGY

2020

Summary of Dissertation

Known colloquially as a killer robot, an autonomous weapon system (AWS), is a robotic weapon. Upon activation, it can decide for itself when and against whom to use force enough to kill. This dissertation will address the issues posed by AWS. The focus will be on AWS that do not feature 'meaningful human control' during times of peace and armed conflict. Thus, unless otherwise stated, in this dissertation, all AWS discussed will be those that do not feature meaningful human control.

There are numerous benefits to AWS. For example, this technology has the potential to save the lives of soldiers charged with menial, dangerous tasks. Furthermore, AWS does not tire, become angry or frustrated and so on. Consequently, civilian lives may be saved by their use also. Additionally, AWS leaves a digital footprint that can effectively track events and bring criminals to justice, and AWS cannot wilfully commit a crime itself.

Nonetheless, AWS may make going to war far too easy and they pose a severe risk to human rights, including the right to life and dignity and the right to a remedy for a victim. The use of force is a key concern. Does AWS comply to international regulations concerning the use of force? Is the technology, a machine with the power of life and death over human beings, compatible with the right to dignity? A gap in accountability may be created in particular by AWS that do not feature meaningful human control and this could then impact the rights of victims to seek the protection of international law.

The legal duty of states under Article 36 of the Additional Protocol I to the Geneva Conventions to review new weapons will be investigated in this dissertation to identify a suitable legal reply to AWS. This duty will also be examined to assess to what extent AWS aligns with recognised standards. According to Article 36, it is required that new weapons be assessed to identify if they are acceptable in relation to several standards, including the human rights system, and whether they result in needless suffering. To begin, this dissertation asserts that AWS that are fully autonomous or have no meaningful human control are not, in fact, strictly weapons. These so-called 'robot combatants' should be dealt with carefully by the international community. After the

elements of Article 36 are understood in detail, it is proposed here that it is appropriate to accept AWS that do not feature meaningful human control.

Regulations of International Humanitarian Law, including precaution, distinction, proportionality rules, are also used to examine AWS. Given that these rules were written to apply to humans and not to machines, which by their very nature cannot exert human judgement, machines will typically fail to satisfy the rules. In addition, the limits of the technology as it exists in the present day and the vague definitions of IHL terms mean that these definitions cannot be transformed into computer code.

In addition, the gap in responsibility created by AWS has the potential to have a negative impact on the rights of victims to pursue a remedy due to the question over who should be held accountable for the actions of AWS. The different types of accountability acknowledged in international law, including command responsibility, corporate, individual and state responsibility, are reviewed in relation to the difficulties posed by AWS. This discussion investigates current proposals for how to resolve these difficulties, including the concept of split responsibility and the argument that command responsibility can be applied to AWS. However, these solutions are found to be impracticable and defective.

This dissertation supports the findings of scholars who argue that meaningful human control can resolve the difficulties associated with AWS. However, international law offers no definition of this term, so jurisprudence concerning the concept of 'control' as a means of determining accountability is used to inform a definition in this dissertation. Tests, which include the strict control test and the effective control test, are discussed to examine ideas around 'dependence' and 'control', which are central to accountability. It is concluded that meaningful human control over a system of weapons can only exist when a human being is responsible for the functions of the system that relate to the selection of a kill target and the decision to execute an action. That is, human input is required for the completion of the most important functions of a weapons system. If that input is absent, the system should be incapable of carrying out these functions.

Abbreviations

ABACUS - Adversary Behaviour Acquisition, Collection, Understanding and Summarization Tool

ACHPR - African Charter on Human and Peoples' Rights

AI- Artificial Intelligence

AP - Additional Protocol

ASR - Draft Articles for State Responsibility

AWS - Autonomous Weapon Systems

CCF - Continuous Combat Function

CCW - United Nations Convention on Certain Conventional Weapons

CEP - Circular Error Probable

CIA - U.S Central Intelligence Agency

CIWS - Close-in Weapon Systems

CLC - International Convention on Civil Liability for Oil Pollution Damage

COIN - Counter Insurgency

DARPA - US Defense Advanced Research Projects Agency

DCDC - Development, Concepts and Doctrine Centre

DMZ - Demilitarized Zone

DoD - Department of Defense

GC - Geneva Convention

GIGO - Garbage In, Garbage Out

HPRC - Program on Humanitarian Policy and Conflict Research

HRW - Human Rights Watch

IAC - International Armed Conflict

IAI - Israel Aerospace Industries

ICC - International Criminal Court

ICCPR - International Covenant on Civil and Political Rights

ICCPR - International Covenant on Civil and Political Rights

ICJ - International Court of Justice

ICL - International Criminal Law

ICRC - International Committee of the Red Cross

ICTR - International Criminal Tribunal of Rwanda

ICTY - International Criminal Tribunal of the Former Yugoslavia

IED - Improvised Explosive Device

IHL - International Humanitarian Law

IHRL - International Human Rights Law

ISIS - Islamic State of Iraq and the Levant

ISR - Intelligence, Surveillance and Reconnaissance

JCE - Joint Criminal Enterprise

LAW - Lethal Autonomous Weapon Systems

LOAC - The Law of Armed Conflict

MAARS - Modular Advanced Armed Robotic System

MHC - Meaningful Human Control

MoD - Ministry of Defence

MPC - United States Model Penal Code

NATO - North Atlantic Treaty Organization

NGO - Non-Governmental Organization

NIAC - Non-International Armed Conflict

OODA - Observe, Orient, Decide, and Act

PMC - Private Military Contractors

ROE - Rules of Engagement

RPA - Remotely Piloted Aircraft.

RUF - Revolutionary United Front

SCADA - Supervisory Control and Data Acquisition

U.S - United States of America

UAV - Unmanned Aerial Vehicle

UCAV - Unmanned Combat Air Vehicle

UDHR - Universal Declaration on Human Rights

UN - United Nations

UUV - Unmanned Underwater vehicle

UWS - Unmanned Weapon System

VCLT - Vienna Convention on the Law of Treaties

Contents

Background 11
Key Definitional Issues 12
Research Question 16
Rationale 16
Methodology 17
Chapter 1 - Autonomous Weapons 19
Introduction 19
Definitions, Distinctions or Features of Autonomous Weapon Systems 19
Unmanned Weapon Systems (UWS) 20
Autonomous Weapon Systems (AWS) 21
Meaningful Human Control (MHC) 22
Critical Functions 23
Humans in the Loop, On the Loop, Out of the Loop 25
The Rules on the Conduct of Hostilities 29
Substantive Obligations 29
Standard of Precautions 30
Bearers of Obligations 32
Conclusion 33
Chapter 2 - The Compliance of Autonomous Systems with International Humanitarian Law 37
Introduction 37
Can AWS Be Deployed in Compliance with the Principle of Distinction? 40
Persons 41
Active Combatants 41
Civilians and Other Protected Persons 45
Civilians Not Protected from Direct Attack 48
Persons Hors de Combat 51
Objects 53
'Nature' and 'Location' 54
'Purpose' and 'Use': The Problem of 'Dual-Use' Objects 57
The 'Definite Military Advantage in the Circumstances Ruling at the Time' 61
Civilian Objects and Specifically Protected Objects 63
Will AWS be Able to Sense Targeting 'Doubt'? 69

Summary 73
Guaranteeing AWS Compliance with LOAC: Using Dynamic Diligence 73
Interaction Between Human and Machine 74
Periodic Assessment 77
Dynamic Operational Limits 78
Conclusion 83
Chapter 3 – Can AWS be Deployed in Compliance with the Principle of Proportionality and with Adequate Precautions? 86
Introduction 86
Autonomous Attacks 88
How an Attack is Defined 91
Acts of Violence 94
Scale 95
Severity 98
Against the Adversary 99
Whether in Offence or in Defence 100
Application to Delayed-Action Weapons 101
Mines 101
Cyberattacks 103
Cyber Hacking, Ruses and Human Accountability 106
Applying Current Law to AWS 111
The Evolution of Targeted Killing 111
Identifying the Attack 114
Summary 127
Potential Solutions 128
Legal Use of AWS 131
Conclusion 143
Chapter 4 - Prohibition of Indiscriminate Weapons and Prohibition of Weapons Causing Unnecessary Suffering, Superfluous Injury 145
Introduction 145
Is it Possible to Define an AWS in the Strictest Sense of the Term 'Weapons' for the Purposes of Article 36 Review? 148
What are the 'Means of Warfare' or the 'Methods of Warfare'? 148
Defining Weapon, Means of Warfare and Methods of Warfare 152

What is a Weapon? 152
Implications of Weapons Autonomy for Legal Analysis 157
Superfluous Injury and Unnecessary Suffering 159
Content of The Principle 159
Application to Autonomous Weapon Systems 161
Prohibition of Weapons Which are Indiscriminate in Nature 167
Content of The Principle 167
Application to Autonomous Weapons Systems 170
Protected Persons and Objects 175
Conclusion 177
Chapter 5 - Autonomous Weapon Systems and Legal Review of New Weapons 179
Introduction 179
The Legal Obligation to Conduct Legal Reviews of New Weapons 179
Customary Law 179
Treaty Law 180
Article 36 Scope of Application 181
State Weapon Review Procedures – Article 36 186
Australia 188
New Zealand 188
The Netherlands 190
Norway 191
Sweden 191
Switzerland 192
United Kingdom 193
United States 194
Similarities Between State Review Procedures 195
Suggested State Review Practices 195
Conclusion 197
Chapter 6 - The Responsibility of States for Internationally Wrongful Acts 199
Introduction 199
State Responsibility 199
AWS and the Law of State Responsibility 201
Unclear Attribution: Private Military Contractors 204

Contracting Phase 205
Recent Developments in the International Legal Framework 206
Including AWS within the ASR Framework 211
AWS Conduct and State Responsibility 211
State Organ Operators and Responsibility 212
Preventing Violations as a Due Diligence Obligation 213
The Removal of Human Judgement 216
Classifying AWS as State Agents 218
Can a Stricter Liability Regime Overcome Potential Accountability Gaps? 222
Accountability in Domestic Courts 224
Conclusion 229
Chapter 7 - Individual Responsibility and Autonomous Weapon Systems 232
Introduction 232
AWS Programmer Liability 233
Armed Conflict as a Threshold Requirement 234
Principal and Accessorial Liability 236
Ex Ante Aiding and Abetting: International Legal Theory 238
The Application of the Effective Control Test within the Robotic Context 240
The Requirement for Mens Rea 249
Summary of Programmer Responsibility 252
The Doctrine of Command Responsibility: A Poor Fit to Govern Artificial Intelligence Systems 253
AWS and the Irrelevance of Command Responsibility 260
Manufacturer Responsibilities for AWS 266
Manufacturers and International Law 266
Criminal Responsibility of Manufacturer 268
Civil Responsibility of Manufacturer 269
Manufacturer Responsibility for AWS Design 270
The Paradox of a Responsible Arms Maker 271
Manufacturer Responsibility for AWS Sale and Supply 271
Manufacturer Responsibility for AWS Use 272
Product Liability 275
No-Fault Liability 277
Summary 278

Conclusion 279
Conclusions and Recommendations 282
Bibliography 289

Background

Autonomous weaponry is a generally recognized generic phrase that incorporates a number of frequently very high technology inventions that have significantly changed the face of the modern battlefield. Autonomous weapon systems (AWS), including completely automated missile systems and robotic ground vehicles, have raised numerous ethical, legal, and wider human rights issues that this dissertation identifies and explores. [1] The widely acknowledged principles of international law that have been highly influential in the shaping of contemporary international humanitarian law now require careful re-examination given the way in which AWS has the potential to revolutionize future conflicts.[2]

These highly important questions have profound significance for global developments in future. We can examine these questions by referring to a continuously expanding and (from the point of view of IHL) disturbing corpus of military encounters in which AWS made a significant difference to the way in which strategies were formulated.[3] From the point of view of commanders, AWS mitigates the need to put human resources in danger, and increases the technical accuracy of both offensive and defensive capabilities. If we accept that military conflict is an inevitable part of human society, it is clearly appealing to find ways of running such conflicts that will reduce the number of deaths involved. [4] The analogy of Kanwar is useful in this context: he explains that in the same way in which a knife gives the human hand greater range and more lethal power, highly technological weapons, e.g. drones, should be regarded as, '… extensions of human action, and the primary difference is the increase in time and distance intervening between the action and result…'[5]

[1] Kenneth Anderson and Matthew Waxman, 'Law and Ethics for Autonomous Weapon Systems: Why a Ban Won't Work and How the Laws of War Can' (2013) Stanford University, The Hoover Institution (Jean Perkins Task Force on National Security and Law Essay Series), [Online] Available < http://dx.doi.org/10.2139/ssrn.2250126>, 3.
[2] Vik Kanwar, 'Post-Human Humanitarian Law: The Law of War in the Age of Robotic Warfare' (2011) 2 *Harvard Journal of National Security* 3, 4.
[3] Eric Jensen, 'The Future of the Law of Armed Conflict: Ostriches, Butterflies, and Nanobots' (2014) 35 *Michigan Journal of International Law* 253, 256.
[4] Rebecca Crootof, 'The Killer Robots Are Here: Legal and Policy Implications' (2015) 36 *Cardozo Law Review* 1837, 1840.
[5] Vik Kanwar, 'Post-Human Humanitarian Law: The Law of War in the Age of Robotic Warfare' (2011) 2 *Harvard Journal of National Security* 5.

However, what appears to be the greatest point in favour of AWS as opposed to standard combat is regarded by many analysts as being his greatest drawback. AWS promotes the concept that by being more precise (i.e. being able to carry out surgical strikes)[6] both military and civilian lives will be saved, making warfare a more ethical process.[7] Many analysts and policymakers reject this, regarding AWS as a significant threat to the dignity of humanity. This research proposal is particularly concerned with three of these threats: firstly, that the intrinsic value of human life will be cheapened if machines are able to make life and death decisions over people;[8] secondly, that there is always the danger of technical malfunction so that human beings will no longer be in control of the killing process;[9] and thirdly, that the asymmetry inherent in AWS, i.e. that it lowers the risk to the attacker and increases the risk to those targeted, is inherently unequal.[10]

Although military commanders may embrace AWS on the basis that it can cut their personnel losses, those who oppose AWS suggest that it may encourage commanders to deploy disproportionate/indiscriminate force against opposition military or civilian targets knowing there is no risk to themselves.[11] Such critics suggest that accidental casualties for civilians will be an inevitable element of AWS deployment.[12]

Key Definitional Issues

This research must also address important issues related to definitions. Chengeta proposes a simple definition of AWS: machines that, when activated, can take decisions regarding the deployment

[6] Paulo Santos, 'Autonomous Weapons and the Curse of History' (2015) *Bulletin of the Atomic Scientists* [Online] Available: < http://thebulletin.org/autonomous-weapons-civilian-safety-and-regulation-versus-prohibition/autonomous-weapons-and-curse-history> [4 November 2016].
[7] Peter Asaro, 'On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-making' (2013) 94 *International Review of the Red Cross* 11, 12.
[8] Peter Asaro, 'On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-making' (2013) 94 *International Review of the Red Cross* 9.
[9] Geneva Academy, *Autonomous Weapon Systems under International Law* (2014) [Online] Available: <http://www.geneva-academy.ch/docs/publications/Briefings%20and%20In%20breifs/Autonomous%20Weapon%20Systems%20under%20International%20Law_Academy%20Briefing%20No%208.pdf> [4 November 2016], 5.
[10] Marco Sassòli, 'Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified', (2014) (90) *International Law Studies, Naval War College*, 310.
[11] Michael Schmitt and Eric Widmar, 'On Target': Precision and Balance in the Contemporary Law of Targeting' (2014) 7 *Journal of National Security and Policy* 379, 381-385.
[12] Louise Arimatsu and Michael Schmitt, 'Attacking 'Islamic State' and the Khorasan Group: Surveying the International Law Landscape' (2014) 53 *Columbia Journal of Transnational Law Bulletin* 1, 3-6.

of weapons with no additional human input.[13] There is as yet no generally agreed legal definition,[14] but all the sources quoted in this proposal are in agreement that what separates AWS from other new military technology is the ability of the system to operate without meaningful human control.[15] This point is exemplified by unmanned aerial vehicles (UAVs, a.k.a. drones). Drones are regarded as semi-autonomous weapons as at present they do not have the capacity to '… select and engage targets without further intervention by a human operator.'[16] Nevertheless, there are examples of drone deployments that illustrate the distinction between semiautonomous weaponry and AWS and the difficulties that arise when military commanders place faith in weaponry that reduces meaningful human control but does not eliminate it. The widely recognized effect of US drone strikes on Taliban forces in Afghanistan illustrates that highly sophisticated weapon systems do not necessarily correlate with perfect precision in targeting.[17]

Crootof details how a number of international organizations joined forces by 2014 in order to call for a global ban on AWS.[18] She contends that although these organizations had praiseworthy aims, i.e. a better definition of AWS' position under IHL, there were fundamental flaws in their approach. She contends that any regulation of AWS up to and including a global ban is not achievable unless we can coherently define what AWS are.[19] The central problem in this area is to define what we mean by autonomy in terms of weapon systems. The definition of the term very much depends on the viewpoint of the stakeholder, and Crootof accurately notes that '… state representatives,

[13] Thompson Chengeta, 'Defining the Emerging Notion of 'Meaningful Human Control' in Autonomous Weapon Systems (AWS)' (2016) [Online] Available: <https://ssrn.com/abstract=2754995> [4 November 2016], citing US Department of Defense Autonomy in Weapon Systems, Directive 3000.09 (2012) [Online] Available: <http://www.dtic.mil/whs/directives/corres/pdf/300009p.pdf> [4 November 2016].
[14] Aaron Johnson, 'The Morality of Autonomous Robots' (2013) 134 *Journal of Military Ethics* 134, 135-138.
[15] Christof Heyns (United Nations), 'Joint report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association and the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions on the Proper Management of Assemblies', A/HRC/31/66, (2013), [67].
[16] Geneva Academy, *Autonomous Weapon Systems under International Law* (2014) [Online] Available: <http://www.geneva-academy.ch/docs/publications/Briefings%20and%20In%20breifs/Autonomous%20Weapon%20Systems%20under%20International%20Law_Academy%20Briefing%20No%208.pdf> [4 November 2016], 6.
[17] Ryan J Vogel, 'Drone Warfare and the Law of Armed Conflict' (2011) 39(1) *Denver Journal of International Law and Policy* 101, 108, 109.
[18] Rebecca Crootof, 'The Killer Robots Are Here: Legal and Policy Implications' (2015) 36 *Cardozo Law Review* 1840.
[19] Rebecca Crootof, 'The Killer Robots Are Here: Legal and Policy Implications' (2015) 36 *Cardozo Law Review* 1840.

developers, military lawyers, human rights activists, philosophers, and other policymakers often talk past each other…'[20]

The fact that AWS are being deployed in contemporary military actions makes this project timely, relevant to general concepts of international law, and offers the opportunity to make an important contribution to the ongoing global debate. Because of this, the design of research for this dissertation and its analysis will be shaped by four separate but linked themes. The first of these themes is concerned with technology, in which the definition of autonomy in terms of modern weapons systems deployment will help to explain the contemporary state of development in this technology. The ways in which the technology continues to grow will obviously influence the development of AWS technology in future.

This theme will be examined in two ways: firstly, by examining what is state-of-the-art in AWS; and secondly, by examining the ways in which technological development can influence what human input there is in the operation of weapon systems. Exploring this theme offers a good basis from which we can go on to explore more complex issues of legal and human rights related to AWS. It should be noted that IHL mandates (particularly the Additional Protocol I to the Geneva Conventions) that all states investigating or developing new weaponry are directly obliged to make decisions as to whether such weaponry is prohibited under IHL.[21]

The second theme for this research incorporates ethics, legal philosophy, and technology, focusing on the part of humans play in taking the decision to use lethal force. It will address the question as to whether a human being can ethically and/or legally ever leave the decision on killing another human being up to a machine or similar autonomous system, and examine whether IHL is suitable for coping with this new reality.[22] IHL must be carefully reconsidered in the context of AWS and

[20] John Lewis, 'The Case for Regulating Fully Autonomous Weapons' (2015) 124 *Yale Law Journal* 1309, 1310-1315.
[21] Additional Protocol I to the Geneva Conventions, Article 36.
[22] A point taken from Jeremy Sarkin, 'The Historical Origins, Convergence and Interrelationship of International Human Rights Law, International Humanitarian Law, International Criminal Law and Public International Law and Their Application from at Least the Nineteenth Century' (2008) *Human Rights and International Legal Discourse, Vol. 1,* [Online] Available: <http://ssrn.com/abstract=1304613> [29 September 2016], 3-5.

the question of whether machines should ever have control, or even an input into control, on the battlefield must be examined.

This leads us automatically to the third theme, the question of whether IHL and AWS can ever be compatible. Risk-free warfare (so-called) in which the chief combatants are not humans may upset the foundational balance of IHL. The last theme of investigation for this research is how we can arrive at a comprehensive definition of legal responsibilities related to AWS, both in terms of political leadership, military command, and decision taking by individuals on the battlefield. It is acknowledged that doctrines of responsibility are multifaceted, e.g., the way in which external powers have international responsibilities for wrongful conduct on the part of secessionist movements.[23] When AWS is deployed by international organizations, it has been proposed that these responsibilities of the type that should be considered in this work.

This research is predicated on the assumption, supported by the first three main themes, that the contemporary framework of IHL needs complete reconsideration in the light of AWS. This will be expanded upon in relation to the fourth theme which will examine the legal responsibility of a state as it develops and deploys AWS. An equally important element of the dissertation is the way in which guarantees can be offered that states will be held to account for the risks they take in deploying AWS.

There are many interesting elements of this last research theme. It cannot be denied that it would be desirable to establish a new world order which regulated the development and deployment of AWS in any future engagements. Nevertheless, as such a large group of states have developed so many different interpretations and definitions of AWS and related law, it does not appear hopeful that there are any international initiatives, of whatever strength or detail, that will be able to stop AWS becoming a central feature of the battlefield in future.[24] As Corn states, future initiatives will

[23] As discussed in Stefan Talmon, 'The Various Control Tests in the Law of State Responsibility and the Responsibility of Outside Powers for Acts of Secessionist Entities' (2009) 58 *International and Comparative Law Quarterly* [Online] Available: <https://ssrn.com/abstract=1402324> [4 November 2016], 4.
[24] Michael Schmitt, 'Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics' (2012) *Harvard National Security Journal Features* 1, 5-6.

be a matter of 'managing the inevitability that weapons will continue to evolve with ever-reduced meaningful human control.' [25]

The greatest difficulty with persuading the international community to implement legislation that will effectively control AWS lies in the too-often-proved fact that it is extremely difficult to persuade all states to come together to develop an agreed legal framework. Even were such general agreement to be achieved and ratified by every state, the Security Council would still potentially provide a significant stumbling block; it is not clear whether the Permanent Members would be willing or able to agree on effective timely sanctions for transgressions of AWS agreements in future. Both the Security Council and the International Criminal Court, and indeed other human institutions, have repeatedly demonstrated that they do not always have the power or the inclination to implement IHL in an effective manner.[26]

Research Question

In line with the four themes of the project detailed above, this research will address the following three questions: a) what forms of AWS must come under the aegis of a comprehensive international legal definition of such weaponry; b) in line with extant norms of international law, what additional laws are required to provide effective regulation for the development and deployment of AWS; and c) how can states be made to take responsibility for enforcing AWS regulations and what sanctions will they face for non-compliance.

Rationale

As suggested by the background information already detailed, AWS has made significant changes to the conduct of modern warfare. This technology does not automatically fit into current IHL frameworks or generally acknowledged rules of war. The technology cannot now be 'put back in the box'. It is inevitable that states will continue to develop and deploy AWS in their desire to create stronger and swifter military deployments while lessening the numbers of human casualties on their side. This research therefore makes a contribution to the current debates regarding the

[25] Geoffrey Corn, 'Autonomous Weapon Systems: Managing the Inevitability of 'Taking the Man out of the Loop'' (2014) [Online] Available: <http://ssrn.com/abstract=2450640> [29 September 2016], 1-2.
[26] Consistent with the UN Charter provisions discussed above.

ways in which human life is taken in military departments from a point of view of ethics, proportionality, and responsibility. An essential element of this research will be to devise a workable definition of AWS in order to deal with the vital questions Crootof raises.

Another purpose of this dissertation will be to help create practical ways of regulating such weaponry, given that it is already so widely disseminated that a ban would be ineffective and/or unworkable. These alternatives could incorporate the creation of codes of conduct for AWS based on accepted ethical and legal principles regarding weaponry and warfare.[27]

Methodology

A case can be made for using any/all of quantitative, qualitative, or mixed methodologies in approaching the question central to this dissertation. [28] This general summary of methodology will include the research approaches detailed below that are especially useful with regard to the already-identified issues of IHL and IHRL. Employing a number of perspectives for examination of this topic will enhance the research outcomes. One example is that exploring the contrast between socio-legal and doctrinaire ('black letter law')[29] in a way that could provide more insight into AWS is central to the planning of this dissertation, with its foundation in the indicative sources noted in the Bibliography. As this area of international law is swiftly developing and driven by technological advances, it is clearly gathering information from questionnaires, personal interviews, AWS technical documents, etc., will all make extremely useful sources for research and help this research to be a useful contribution to the literature.[30]

Although quantitative methodologies would undoubtedly be useful, they will not be used for this dissertation due to the fact that a) to be carried out effectively would require relatively costly inputs in terms of drafting, creating, and undertaking data collection, and b) there is so much primary

[27] Kenneth Anderson and Matthew Waxman, 'Law and Ethics for Autonomous Weapon Systems: Why a Ban Won't Work and How the Laws of War Can' (2013) Stanford University, The Hoover Institution (Jean Perkins Task Force on National Security and Law Essay Series), [Online] Available < http://dx.doi.org/10.2139/ssrn.2250126>, 2.
[28] Jennifer Rowley, 'Using Case Studies in Research' (2002) 25(1) *Management Research News* 16, 20.
[29] Paul Chenowyth, 'Legal Research' (2012) Salford University [Online] Available: <http://www.csas.ed.ac.uk/__data/assets/pdf_file/0005/66542/Legal_Research_Chynoweth_-_Salford_Uni.pdf> [4 November 2016], 29, 30.
[30] A point taken from *New York University* 'What is Research Design' (2014) [Online] Available: <www.nyu.edu/classes/bkg/methods/005847ch1.pdf> [29 September 2016], 2-3.

source documentation available (especially regarding contemporary international law and case histories), alongside much high-quality research literature that can be reviewed for research into IHL and AWS that it alone is sufficient for a high-quality piece of research work with relevant recommendations and conclusions.[31] For both of these reasons, this research will employ a qualitative methodology. Given that more than 100 peer-reviewed articles have appeared related to AWS/IHL matters from 2014 onwards, the only real qualitative research challenge currently identified is the selection of the most apposite sources.

[31] As suggested from reading (i) John Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th edn, Sage, 2013), 18, 21, and 23-30; (ii) Gina Peruginelli, 'Evaluating Research: the Case of Legal Scholarly outputs' (2015) 14(2) *Legal Information Management* 50.

Chapter 1 - Autonomous Weapons

Introduction

International lawmakers have been experiencing an increasingly prominent level of concern over the past ten years in view of the emergence of technologically sophisticated autonomous weapon systems (AWS). This stems from the fact that these devices are programmed with the capability to kill human targets without the need for human orders, thus underscoring the contemporary relevance of the idea that 'technology is a double-edged sword'.[32] While some in the international community emphasise the significant degree to which AWS have the capacity to conserve human life (thereby transforming the nature of armed conflict for the good), others argue that these systems disregard some of the fundamental rights that humans have. Ultimately, although AWS are still being developed and, moreover, have not yet been applied in the context of armed conflict, the matter of determining their legality or illegality is a difficult task, primarily because it would mark their deployment ethical or unethical upon becoming available. Hence, reservations of this kind have contributed to a situation in which lawmakers, international agencies, and legal scholars are unsure of how to view the eventual emergence of AWS.

The purpose of the present research is to identify whether AWS are illegal weapons and, in the event that they are determined not to be, to outline the situations under which their use could potentially infringe on the existing legal framework. Notably, this will inform the researcher as to the degree to which International Humanitarian Law rules are sufficient to regulate the utilisation of AWS. To achieve this purpose, it will first be necessary to outline the key terms drawn on in this research, and so that is the primary concern of this chapter.

Definitions, Distinctions or Features of Autonomous Weapon Systems

It will be useful to outline the various designations used to refer to (what up to now have been called) AWS, especially prior to defining what the technology and its related terms are. In certain contexts, the term 'lethal autonomous robots' is used, while other commonly encountered terms

[32] 'We have to realize that science is a double-edged sword. One edge of the sword can cut against poverty, illness, disease and give us more democracies, and democracies never war with other democracies, but the other side of the sword could give us nuclear proliferation, bio-germs and even forces of darkness.' See Michio Kaku, *The Future of the Mind: The Scientific Quest to Understand, Enhance, and Empower the Mind* (Overseas Editions New, 2014) 17.

include ‘lethal autonomous weapon systems’ (LAW), ‘killer robots’, and, as used in this research, ‘autonomous weapon systems’ (AWS).

The argument against using a term such as ‘killer robots’ is relatively straightforward. Its use implies that the weapon system in question has human-like qualities and a level of intelligence comparable to humans (as though a ‘terminator’ or ‘Robocop’), but this is far from the truth because general AI has yet to be developed.[33] It is this term’s potentially misleading nature as to the actual capabilities of the system in question that has resulted in it being discredited by many scholars,[34] along with the possibility that the irrational fears it gives rise to could influence decision-making. As for terms which draw on the word ‘lethal’ to designate these types of emerging technologies, including ‘lethal autonomous weapon systems’ (LAW), the United Nations Special Rapporteur on extrajudicial, summary, or arbitrary executions demonstrated that this places unhelpful constraints on the debate.[35] Although the lethality of the system in question is an important matter that must be debated, it ought to be debated alongside the more wide-ranging issue of the deployment of autonomous machines that have the capacity to cause harm and use force. The term autonomy is derived from the Greek words auto (self) and nomos (law) and is used to infer self-governing or self-rule.[36] When applied within the context of weapons, the use of this term indicates that a weapon can self-govern; that is, it does not need human intervention to activate. Therefore, a convenient term to use for the purposes of the present research is ‘autonomous weapon systems’ (AWS).

Unmanned Weapon Systems (UWS)

UWS are weapon systems, designed to apply force for the purpose of causing harm in armed conflicts, which do not require human operators. As such, they act either in an independent manner or, alternatively, they are directed from a distance (i.e., remotely controlled). Typical examples of

[33] Peter Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (Penguin Reprint edition, 2009) 101.
[34] A/HRC/23/47, Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Christof Heyns, 9 April 2013, 8.
[35] A/HRC/23/47, Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Christof Heyns, 9 April 2013, 8.
[36] Armin Krishnan, *Killer Robots: Legality and Ethicality of Autonomous Weapons* (Ashgate Publishing 2009) 15, 19.

UWS[37] include autonomous or remotely controlled ground or aircraft systems which lack human operators and, moreover, which offer a degree of utility when deployed in combat (i.e., transporting pay-loads, whether lethal or non-lethal).[38]

Autonomous Weapon Systems (AWS)

Despite the lack of a universal definition of AWS in the international legal community,[39] the following features of AWS have been collected into a working definition that is typically acknowledged and used as the basis of debates: firstly, AWS are robotic[40]; secondly, they are unmanned; and thirdly, upon activation, they can independently identify and facilitate engagement with a target.[41] AWS have distinct features when comparatively examined against remotely controlled UWS.[42] For instance, the defining feature of AWS in this sense is that the machines themselves is programmed to oversee, monitor, and guide their navigation, tracking, targeting, and decision-making, all without the need for human intervention.

The overarching category of AWS can be further subdivided into the following: firstly, 'semi-autonomous weapon systems'; secondly, 'supervised autonomous weapon systems'; and thirdly,

[37] 'One of the most common uses of UWS's in both military and civilian capacities is to simply provide surveillance and reconnaissance. Currently the Predator and the Hunter are frequently deployed in combat situations.' Maziar Arjomandi, *Classification of Unmanned Aerial Vehicles* (2007) course material for Mechanical Engineering 3016, the University of Adelaide, Australia 34.

[38] See US Department of Defence Dictionary of Military and Associated Terms (2001) 579.

[39] For a report of the first meeting see: ICRC (2014) Autonomous Weapon Systems Technical, Military, Legal and Humanitarian Aspects, Report of an Expert Meeting held 26-28 March 2014 (published November 2014), https://www.icrc.org/en/download/file/1707/4221-002-autonomous-weapons-systems-full-report.pdf (accessed 30 October 2017).

[40] AWS can be perceived to be a robot or a machine since both these objects are created by humans. All robotic systems, including autonomous weapon systems, include three elements: 1) the system that the programmers bestow with instruments, 2) a processor or other form of artificial intelligence that makes a decision how to respond to a given event, and 3) executions that take action in accordance with a decision made by a human operator or the machine itself. Peter Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (Penguin Reprint edition, 2009) 67.

[41] See A/HRC/23/47, Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Christof Heyns, 9 April 2013, 7. The report cites almost similar definitions provided by the US Department of Defence and Human Rights Watch; See also the US Department of Defense Autonomy in Weapon Systems, Directive 3000.09 (2012) available at http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf (accessed 3 November 2017).

[42] An example is a combat drone, sometimes called an Unmanned Aerial Vehicle (UAV) or Unmanned Air System (UAS) which is 'an unmanned aerial aircraft [or ground system] that does not carry a human operator but is piloted remotely and [carries] a lethal payload.' See US Department of Defence *Dictionary of Military and Associated Terms* (2001) 579.

'fully-autonomous weapon systems.'[43] This research concentrates on AWS which are not associated with 'Meaningful Human Control', namely, which have the capacity to engage and kill targets in a wholly independent and autonomous manner.

Meaningful Human Control (MHC)

The uncertainty surrounding what represents the legal application of AWS naturally extends to methods of ensuring that the use of AWS remains within legal limits. Apprehensions related to this issue are derived from concerns that humans are increasingly relinquishing control of weapon systems to computers. As such, one of the most common elements of the AWS debate to date concerns the concept of maintaining 'meaningful human control' (MHC) over AWSs. This idea refers to concerns that, if an AWS has a capacity for autonomous operation, it may develop the ability to operate beyond the control of the armed forces and, as such, the level of autonomy that is built into systems of this nature must be limited to a certain degree to ensure they consistently function according to moral and legal requirements.

There is a lack of consensus as to what represents meaningful human control. State X could perceive meaningful human control to necessitate informed human approval of every action that a weapon system can take and, thereby, ensure that humans remain in the loop throughout the process. However, State Y might view it as the ability of a human to supervise and prevent the actions of a weapon system and, therefore, be in the loop; and State Z might be of the opinion that the original programming alone should offer sufficient meaningful human control of the extent to which humans do not need to be in the loop.[44] However, the Czech Republic is firmly of the opinion that 'the decision to end somebody's life must remain under meaningful human control, . . . [t]he challenging part is to establish what precisely meaningful human control would entail.'[45]

[43] US Department of Defense Autonomy in Weapon Systems, Directive 3000.09 (2012) available at http://www.dtic.mil/whs/directives/corres/pdf/300009p.pdf (accessed 3 November 2017).
[44] Rebecca Crootof, 'A Meaningful Floor for Meaningful Human Control' (2016) *Temple International and Comparative Law Journal* 53.
[45] Statement of the Czech Republic, CCW Meeting of Experts on Lethal Autonomous Weapons Systems, Geneva, April 13-17, 2015, http://www.unog.ch/80256EDD006B8954/(http Assets)/2DD5110A33C9C2D2C1257E26005DD47B/$file/2015_LAWS_MX_Czech+Republic.pdf.

Given MHC's status as a novel term recently formulated by Article 36, a non-governmental organisation[46], it should be recognised that there is no formal definition of the term in the context of international law. Therefore, for the purposes of the present research, MHC is defined in relation to the level of direction a human operator (in this case, a soldier) has over the 'critical functions' of a weapon system, to the degree that they and their real-time input – as opposed to the weapon system itself – constitute the key determinants of the system's operation and 'critical functions'.

Critical Functions

The 'critical functions' of a weapon system are those which are related in a direct way to the tracking, selection, and eradication of targets.[47]

The Difference between 'Autonomy' and 'Automation' Weapon Systems in Fact

In order to distinguish between "autonomous" and "automated"; decision-making capabilities and the amount of adaptation are key factors. On the one hand, an autonomous system learns, evolves, and adapts to dynamic environments. On the other hand, automated systems in most cases perform within a pre-defined set of parameters and have been restricted in how they can perform and what tasks they can perform. As a case in point, certain systems upon activation can engage and kill human targets without the need for operator supervision, while others' design features require that operators are present. It is worth noting that referring to the latter as autonomous in any respect is misleading, and so it is evident that a sophisticated definition of what autonomy in weapon systems denotes is required. As stated by W.C. Marra in a discussion centring on machine and weapon systems, autonomy arises as the product of the variables of 'independence', 'adaptability', and 'discretion'. Moreover, a system's level of autonomy should be considered on the basis of the following issues:

[46] 'a positive obligation in international law for individual attacks to be under meaningful human control … it is moral agency that [the rules of proportionality and distinction] require of humans, coupled with the freedom to choose to follow the rules or not, that are the basis for the normative power of the law.' Article 36, 'Killer Robots: UK Government Policy on Fully Autonomous Weapons' (Policy Paper, April 2013) 1 <http://www.article36.org/wpcontent/uploads/2013/04/Policy_Paper1.pdf?con=&dom=pscau&src=syndication>

[47] See Report of the ICRC Expert Meeting on 'Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects', 26-28 March 2014, Geneva, available at https://www.icrc.org/en/document/report-icrc-meeting-autonomous-weapon-systems-26-28-march-2014

'A system is autonomous when it acts with infrequent operator interaction, when it is able to function successfully in unfamiliar environments, and when it achieves mission objectives with a high level of assertiveness. As a result, like intelligence and consciousness, autonomy is best conceived of as existing on a spectrum.[48] *Some machine systems would clearly lie on the automated end, while other systems might be closer to autonomous.'*[49]

In view of this, it is critical to outline the distinction between 'autonomous' weapon systems and 'automated' weapon systems. The latter denotes a weapon system which has been designed for the purpose of operating in a planned environment in an expectable way, while the former can operate in unplanned environments and, moreover, frequently in unexpected ways.

Another point to note about the passage from W.C. Marra cited above is the use of the phrase 'infrequent operator interaction'. The implication of this is that although certain weapon systems may depend on operator control under a given set of circumstances, it can be designated autonomous rather than automated in the event that it acts independently the majority of the time. According to the definition of the International Committee of the Red Cross, autonomous weapon systems are characterised by the lack of MHC over the system's 'critical functions'.[50] The degree to which a machine is autonomous should be evaluated in terms of a range, where a low level of autonomy places the system at the start of the range, while a high level of autonomy places the system at the middle or end of the range (for semi-autonomous and fully-autonomous weapon systems, respectively).

In view of the above discussion, we may conclude that the use of the term 'autonomy' in the context of debates about weapon systems does not relate to the traditional philosophical view of

[48] Grant Clark et al, 'Mind and Autonomy in Engineered Bio-systems' (1999) 12 *Engineering Applications of Artificial Intelligence* 10.
[49]William Marra and Sonia McNeil, 'Understanding "the loop": Regulating the Next Generation of War Machines' (2013) 36 *Harvard Journal of Law and Public Policy* 1155; See also US Department of Defense *Unmanned Systems Integrated Road Map FY 2011-2036* (2011) 44. Available at https://fas.org/irp/program/collect/usroadmap2011.pdf (accessed 28 October 2017).
[50] See Report of the ICRC Expert Meeting on 'Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects', 26-28 March 2014, Geneva, available at https://www.icrc.org/en/document/report-icrc-meeting-autonomous-weapon-systems-26-28-march-2014

self-determination or agency.[51] Instead, a weapon system is autonomous if – based on the operation first given to it by a human – 'A weapon system which, once activated, can select and engage targets without further human intervention and usually without any human pre-selecting those specific targets; and, in the process, to exercise discretion and self-direction to operate in a potentially complex and unstructured environment.'[52]

Humans in the Loop, On the Loop, Out of the Loop

Formulating accurate definitions of what an autonomous system is cannot neglect the notion of a human being 'in', 'on', or 'out of' the loop. The terms human in the loop and human out of the loop were first employed in the context of military affairs,[53] along with computer-based disciplines, following Boyd's formulation of a notable human decision-making framework, namely, the OODA ('observe, orient, decide, and act') loop.[54]

The think-act model which lies at the basis of machine and robot behaviour is founded on the OODA loop, which becomes clear when one considers the stages of data acquisition, data analysis, decision-making, and decision implementation they proceed through.[55] Critically, then, a mistake made at any stage of the loop is highly consequential in informing (or, more accurately, misinforming) the remaining stages of the loop.[56] Owing to this possibility, human operators have typically been kept 'in' the loop (here, the OODA loop) to supervise and confirm the veracity of each stage's outcomes for the machine, and this has particular been the case in the context of life and death decisions.

---

[51] Gerald Dworkin, *The Theory and Practice of Autonomy* (Cambridge University Press, 1988) 6; A/HRC/23/47, Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Christof Heyns, 9 April 2013, p 8, para 43.

[52] Maziar Homayounnejad, 'Assessing the Sense and Scope of Autonomy in Emerging Military Weapon Systems' (August 24, 2017). TLI Think! Paper 76/2017. Available at SSRN: https://ssrn.com/abstract=3027540 or http://dx.doi.org/10.2139/ssrn.3027540 15.

[53] The Marine Corps' War fighting Manual states that the party that completes the OODA loop cycle faster than the other gains the military advantage. Available at http://www.marines.mil/Portals/59/Publications/MCDP%201%20Warfighting.pdf (accessed 18 September 2017).

[54] Frans Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd* (Routledge 1 edition, 2006).

[55] Gilles Coppin and Legras Francois, 'Autonomy Spectrum and Performance Perception Issues in Swarm Supervisory Control' (2012) 100 *Proceedings of the IEEE* 592.

[56] C William et al, 'Understanding "the loop": Regulating the Next Generation of War Machines' (2013) 36 *Harvard Journal of Law and Public Policy* 1148.

In view of this, the extent to which any machine or robot is autonomous has, therefore, been measured by the extent to which it depends on human interaction when engaging in the OODA loop.[57] When UWS require the assistance of human operators to finish the OODA loop, humans are designated as being 'in' the loop, whereas when UWS can complete the loop independently of human operators, humans are designated at being 'out' of the loop.

To summarise, the three levels of autonomy are, among others, defined in the Losing Humanity: The Case Against Killer Robots report issued by Human Rights Watch (HRW), by the US Department of Defense (DoD) in its 2012 Directive on Autonomy in Weapon Systems, as well as by Armin Krishnan in his comprehensive book Killer Robots: Legality and Ethicality of Autonomous Weapons. The distinction they provide are as follows[58]:

Level of Autonomy	HRW	DoD	Krishnan
1	Human-in-the-loop	Semi-autonomous	Pre-programmed autonomy
2	Human-on-the-loop	Human-supervised autonomous	Limited or Supervised autonomy
3	Human-out-of-the-loop	Fully autonomous	Complete autonomy

A UWS is classified as autonomous, semi-autonomous, or automated on the basis of three fundamental considerations, first among which is the degree to which the achievement of its 'critical functions' necessitates the presence of a human 'in' the loop. When a UWS acts in a primarily independent way after it has been activated, then it can be classified as an AWS.[59] In addition to this, the level of success a UWS has in operating within an unplanned and unpredictable

[57] Peter Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (Penguin; Reprint edition, 2009) 74; C William et al 'Understanding "the loop": regulating the next generation of war machines' (2013) 36 *Harvard Journal of Law and Public Policy* 1150.
[58] Human Rights Watch, *Losing Humanity: The Case Against Killer Robots* (November 2012) 2; United States of America Department of Defense Directive 3000.09 on subject "Autonomy in Weapon Systems", 21 November 2012, 13,14; Armin Krishnan, *Killer Robots: Legality and Ethicality of Autonomous Weapons* (Ashgate, 2009) 45.
[59] Armin Krishnan, *Killer Robots: Legality and Ethicality of Autonomous Weapons* (Ashgate, 2009) 4.

context is indicative of the degree to which it is autonomous, where it would be classified as an AWS in the event that it can successfully react to unexpected scenarios.[60] Finally, the autonomous or automated distinction is determined in relation to the ability a UWS has in asserting its operational decisions when executing its 'critical functions'. If the UWS in question demonstrates discretion in the context of its decision-making and decision implementation, then it is placed further towards the autonomous end of the spectrum as opposed to the automated end. UWS which are autonomous often have the capabilities and resources required to identify alternative ways in which to fulfil specific mission requirements successfully. Hence, we may conclude that an AWS has the resources required to complete its fundamental task without the supervision of an operator,[61] along with the capabilities needed to evaluate, decide on, and implement a certain course of action in unpredictable contexts.[62]

If a weapon system satisfies the above criteria for autonomy, then it has the capability following activation to fulfil its 'critical functions' in an operator-independent manner. Importantly, then, it should be noted that this matter is where the centre of the debate about these technologies lies, where questions revolve primarily around the issue of whether humans are 'in', 'on', or 'out of' the OODA loop, or 'in the wider loop'.[63] According to prominent robotics practitioners such as Arkin, truly autonomous machines are a technological impossibility. To similar effect, the United States has long emphasised that irrespective of the technological viability of truly autonomous machines, human intervention will always be a feature of their utilisation.[64] This is what gave rise to the United States policy that 'autonomous and semi-autonomous weapon systems shall be designed to allow commanders and operators to exercise appropriate levels of judgment over the

[60] C William et al, 'Understanding "the loop": Regulating the Next Generation of War Machines' (2013) 36 *Harvard Journal of Law and Public Policy* 1154.
[61] Armin Krishnan, *Killer Robots: Legality and Ethicality of Autonomous Weapons* (Ashgate, 2009) 5; See also US Department of Defense *Defense Science Board, Task Force Report*, 1; US Department of Defense *Unmanned Systems Integrated Roadmap* (2013) 66, 67.
[62] Troy Jones & Mitch Leammukda, 'Requirements-Driven Autonomous System Test Design: Building Trust Relationships (2010) 1 International Test and Evaluation Association (ITEA) Live Virtual Constructive Conference, El Paso, TX, January 11-14.
[63] A/HRC/23/47, Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Christof Heyns, 9 April 2013, p 8, para 39.
[64] Peter Singer, 'In the Loop? Armed Robots and the Future of War' (2009) 1 quoting a US Air force Captain. Available at http://www.brookings.edu/research/articles/2009/01/28-robots-singer (accessed 10 November 2017).

use of force'.[65] An analogous policy emerged from the United Kingdom context, with the government stating that operator-independent weapons will never be deployed in conflict situations.[66]

Despite the abovementioned policies, several scholars have suggested that practice proves otherwise. As a case in point, US Colonel Adams suggested that while governments are now insisting on the guarantee that humans will never be taken out of the OODA loop, technological change is taking place at such a rate that maintaining humans in the loop will no longer be feasible.[67] Another notable commentator, Shachtman, suggested that the US government's assurances of humans remaining in the OODA loop of UWS is explicitly cynical, namely, in that it serves as a useful way to minimise the public outcry that would otherwise arise.[68]

A weapon can only be perceived to be autonomous if the critical functions by which it uses force that could be lethal are executed autonomously, thereby excluding humans from the loop. In this context, the term 'loop' refers to the process by which a target is selected and a decision as to whether to attack that target is made. This may be limited to the critical processes (target selection and engagement) that the weapon carries out autonomously or the full targeting process within which humans play a decisive role. From the point of view of international humanitarian law, it is logical that the latter interpretation of the term 'loop' should be applied to take into account the various processes that come before the selection of a target and a subsequently attack on it including tasks such as formulating objectives, selecting a target, selecting a weapon, and implementation planning—processes that must also bear in mind the potential consequences that such actions could have on civilian populations.

[65] US Department of Defense (2012) *Autonomy in Weapon Systems, Directive 3000.09*, 21 November 2012, Glossary, Part II Definitions para 4(a).
[66] UK Ministry of Defence (2013) Written Evidence from the Ministry of Defence submitted to the House of Commons Defence Committee inquiry *'Remote Control: Remotely Piloted Air Systems - Current and Future UK Use*', September 2013, 3.
[67] Thomas K. Adams, 'Future Warfare and the Decline of Human Decision-making Parameters' (2001) *U.S. Army War College Quarterly* 57, 58.
[68] Quoted in Peter Singer 'In the loop? Armed Robots and the Future of War' (2009) 2 Available at http://www.brookings.edu/research/articles/2009/01/28-robots-singer (accessed 25 October 2017).

For example, Germany's closing statement at the 2015 CCW conference on autonomous weapons systems, announced that Germany 'will not accept that the decision over life and death is taken solely by an autonomous system without any possibility for a human intervention'.[69] As commentators have noted, this statement 'leaves significant space for requiring different levels of control and for demarcating critical functions that would require high levels of human control from less critical functions that would require lower or no direct human control'.[70]

The Rules on the Conduct of Hostilities

Substantive Obligations

According to the principle of distinction, all parties that are involved in a given conflict must differentiate between combatants and civilians, and military objectives and civilian objects.[71] This principle is reflected in a number of API articles.[72] Legally, attacks are only permissible if they are targeted at combatants and military objectives. Any attacks against civilian objects or civilians are illegal unless the civilian is directly participating in the hostility.

---

[69] Final Statement by Germany, CCW Expert Meeting on Lethal Autonomous Weapons Systems, 13–17 April 2015, Geneva, available at <www.unog.ch/80256EDD006B8954/(httpAssets)/07006B8A11B9E932C1257E2D002B6D00/$file/2015_LAWS_MX_Germany_WA.pdf>.

[70] Nehal Bhuta et al. Eds., *Autonomous Weapons Systems: Law, Ethics, Policy* (Cambridge University Press, 2016) 382.

[71] In its advisory opinion in the Nuclear Weapons case in 1996, the ICJ considered 'the principle of distinction between combatants and non-combatants to be one of the cardinal principles contained in the texts constituting the fabric of humanitarian law and also one of the intransgressible principles of international customary law'. ICJ, Nuclear Weapons case, Advisory Opinion, 8 July 1996, §§ 78–79; In its judgment in the Blaškić case in 2000, the ICTY held that 'the parties to the conflict are obliged to attempt to distinguish between military targets and civilian persons.' ICTY, Blaškić case, Judgment, 3 March 2000, § 180; According to an Inter-American Commission on Human Rights report on the human rights situation in Colombia issued in 1999, 'IHL prohibits the launching of attacks against the civilian population and requires the parties to an armed conflict, at all times, to make a distinction between members of the civilian population and persons actively taking part in the hostilities and to direct their attacks only against the latter and, inferentially, other legitimate military objectives.' Inter-American Commission on Human Rights, Third report on the human rights situation in Colombia, Doc. OEA/Ser.L/V/II.102 Doc. 9 rev. 1, 26 February 1999, § 40; The Rules of International Humanitarian Law Governing the Conduct of Hostilities in Non-international Armed Conflicts, adopted in 1990 by the Council of the International Institute of Humanitarian Law, provides: 'The obligation to distinguish between combatants and civilians is a general rule applicable in non-international armed conflicts.' The commentary on this rule notes that it is based on the St. Petersburg Declaration, Article 25 of the Hague Regulations, UN General Assembly Resolutions 2444 (XXIII) and 2675 (XXV), common Article 3 of the 1949 Geneva Conventions and Article 13(2) of the 1977 Additional Protocol II. International Institute of Humanitarian Law, Rules of International Humanitarian Law Governing the Conduct of Hostilities in Non-international Armed Conflicts, Rule A1 and Commentary, IRRC, No. 278, 1990, Commentary, pp. 387–388; Canada's Use of Force Manual (2008) states: 'In terms of use of force, an essential feature of the LOAC [law of armed conflict] is that it allows for the deliberate use of deadly force against individuals directly participating in hostilities (during international or non-international armed conflicts), whether or not they are presenting a threat at the moment'. Canada, Use of Force for CF Operations, Canadian Forces Joint Publication, Chief of the Defence Staff, B-GJ-005-501/FP-001, August 2008, § 105.6.

[72] API arts 48, 51(2) and 52(2).

The principle of proportionality stresses that any incidental damage that is caused to civilian objects or civilians (based on the information that is realistically available to those who are responsible for planning and managing the attack) must not be excessive in comparison to the 'concrete and direct' military advantage that will be gained from anticipating such an attack.[73]

The legal requirement to warrant that the means and methods that are utilised in the attack are permitted and, on a more general level, the attacker has taken sufficient precautions during the process of planning the attack, represent the process by which the underlying obligations of the principles of distinction and proportionality are adhered to. Article 57 outlines this process; however, it is worth pointing out that 'to some extent Article 57 reaffirms rules which are already contained explicitly or implicitly in other articles',[74] generally those describing the principles of proportionality and distinction, as highlighted above. At a high level, Article 57 asserts that attacks can only be planned and launched against lawful military targets, and that adequate precautions must be taken during the attacks themselves.[75]

Standard of Precautions

Many of the obligations that specifically relate to attacks, in particular, those outlined in Article 57 of API, are articulated in terms of feasibility; for example, attackers are required to 'do everything feasible' to ensure that only military targets are attacked,[76] must 'take all feasible precautions' when selecting the means and methods of attack in order to reduce the risk of incidental harm to civilian objects and civilians,[77] and so on.[78]

[73] API arts 51(5)(b) and 57(2)(a)(iii).
[74] Claude Pilloud and Jean Pictet, 'Protocol I – Article 57 – Precautions in Attack' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 679 [2189].
[75] Ian Henderson, *The Contemporary Law of Targeting* (Martinus Nijhoff, 2009) 12.
[76] API art 57(2)(a)(i).
[77] API art 57(2)(a)(ii).
[78] The US Naval Handbook (2007) states: 'The law of targeting, therefore, requires that all reasonable precautions must be taken to ensure that only military objectives are targeted so that non-combatants, civilians, and civilian objects are spared as much as possible from the ravages of war.' United States, The Commander's Handbook on the Law of Naval Operations, NWP 1-14M/MCWP 5-12.1/COMDTPUB P5800.7, issued by the Department of the Navy, Office of the Chief of Naval Operations and Headquarters, US Marine Corps, and Department of Homeland Security, US Coast Guard, July 2007, § 8.1; UN General Assembly Resolution 2675 (XXV), adopted in 1970, states: 'In the conduct of military operations, every effort should be made to spare civilian populations from the ravages of war, and all necessary precautions should be taken to avoid injury, loss or damage to civilian populations.' UN General Assembly, Res. 2675 (XXV), 9 December 1970, § 3, voting record: 109-0-8-10; In its judgment in the Kupreškić case in 2000, the ICTY Trial Chamber stated that 'Article 57 of the 1977 Additional Protocol I was now part of customary

'Feasibility' serves a utility as both an upper and lower limit on the standard of precautions to be taken. According to the outputs of the 1974-77 Diplomatic Conference, feasibility means 'that which is practical or practically possible taking into account all the circumstances at the time, including those relevant to the success of military operations.'[79] Per this definition, the law takes into consideration the fact that conflict carries with it a risk of civilian harm. However, it expressly requires that adequate mandatory precautions are taken for each instance of an attack that are designed to achieve the balance of humanity and military advantage that is demanded by the IHL. What actions are considered to be feasible and necessary to maintain that balance is 'a matter of common sense and good faith.'[80]

It is worth noting that, during the process by which API was negotiated, it was highlighted that the standards that apply to the identification of objectives 'depended to a large extent on the technical means of detection available to the belligerents. … For example, some belligerents might have information owing to a modern reconnaissance device, while other belligerents might not have this

international law, not only because it specified and fleshed out general pre-existing norms, but also because it did not appear to be contested by any State, including those who had not ratified the Protocol. The Trial Chamber also noted that in the case of attacks on military objectives causing damage to civilians, international law contains a general principle prescribing that reasonable care must be taken in attacking military objectives so that civilians are not needlessly injured through carelessness'. ICTY, Kupreškić case, Judgment, 14 January 2000, § 524; With reference to the Martens Clause, the Chamber held: 'The prescriptions of … [Article 57 of the 1977 Additional Protocol I] (and of the corresponding customary rules) must be interpreted so as to construe as narrowly as possible the discretionary power to attack belligerents and, by the same token, so as to expand the protection accorded to civilians.' ICTY, Kupreškić case, Judgment, 14 January 2000, § 525; Germany's Military Manual (1992) states: 'When launching an attack on a military objective, all feasible precautions shall be taken to avoiding, and in any event to minimizing, incidental losses of civilian life, injury to civilians and damage to civilian objects.' Germany, Humanitarian Law in Armed Conflicts – Manual, DSK VV207320067, edited by The Federal Ministry of Defence of the Federal Republic of Germany, VR II 3, August 1992, English translation of ZDv 15/2, Humanitäres Völkerrecht in bewaffneten Konflikten – Handbuch, August 1992, § 510.

[79] Michael Bothe, Karl Josef Partsch and Waldemar Solf, *New Rules for Victims of Armed Conflicts* (Martinus Nijhoff, 2013) 405; Claude Pilloud and Jean Pictet, 'Protocol I – Article 57 – Precautions in Attack' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 682 [2198].

[80] Claude Pilloud and Jean Pictet, 'Protocol I – Article 57 – Precautions in Attack' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 682 [2198].

type of equipment.'[81] Attackers are legally required to ensure they make full and comprehensive use of the data, information, and technologies that are available to them in the run up to the attack.[82]

Bearers of Obligations

Generally speaking, the requirement to take adequate precautions in relation to a given attack is the direct responsibility of the States, as participants in the conflict, signatories to API, and subjects of international law. However, API also outlines that 'those who plan or decide upon an attack',[83] are obliged to take necessary precautions. As such, individuals, in particular military personnel, are also legally expected to adhere to the requirements of API. During the 1974-77 Diplomatic Conference, some delegates moved to limit this obligation to senior-ranking officials.[84] However, API in its current form does not delineate such restrictions. While it is factual that '[i]n conventional warfare involving large forces of combined arms these functions are generally performed at higher levels of command',[85] this is not necessarily the case in all types of conflict; for example, a conflict that involves some form of guerrilla warfare would represent an exception to this rule. A reading that is more reflective of reality is that 'the obligations apply at whatever level the regulated functions are being performed.'[86] However, there are some proponents of the notion that 'higher the level [of command] the stricter the required compliance is.'[87]

As per Article 57, all feasible efforts must always be made to protect civilian objects and individuals.[88] The Article's use of the passive mood shows that any individual with influence upon automated or autonomous attacks is obliged to exercise this protection and under no circumstances

[81] Claude Pilloud and Jean Pictet, 'Protocol I – Article 57 – Precautions in Attack' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 682 [2199].
[82] Ian Henderson, *The Contemporary Law of Targeting* (Martinus Nijhoff, 2009) 162.
[83] API art 57(2)(a).
[84] e.g. Switzerland, Austria, New Zealand; Ian Henderson, *The Contemporary Law of Targeting* (Martinus Nijhoff, 2009) 160.
[85] Michael Bothe, Karl Partsch and Waldemar Solf, *New Rules for Victims of Armed Conflicts* (Martinus Nijhoff, 2013) 405.
[86] Alexandra Boivin, 'The Legal Regime Applicable to Targeting Military Objectives in the Context of Contemporary Warfare' (2006) Research Paper Series No 2/2006 University Centre for International Humanitarian Law i.
[87] Jean-Marie Henckaerts and Louise-Doswald Beck, *Customary International Humanitarian Law* (Cambridge University Press, 2005) vol. 2, 359.
[88] API, Article 57(1).

exempted of this responsibility.[89] Within the realms of automated and autonomous attacks, this implies that software developers, those who upload mission data to weapon control systems, mission planners, authorising officers, platform operators who oversee missions and any individual processing mission-critical data, be the resulting decisions human- or system-made, are duty-bound to exercise maximum care towards civilian objects and individuals.

Considering an automated or autonomous attack, the concept of planners would, naturally, include sortie-specific planners. Logically, developers of target recognition software would also be responsible for ensuring, as best possible, that such weapon systems recognise only legal targets. A narrow definition of planning would not seem appropriate for such a context. Regardless, this obligation for planners to exercise maximum care is a simple development of their existing obligation to make all possible efforts to protect civilians. This rule would seem to impose certain responsibilities on planners using autonomous or automated attack systems, as well as their unit commanders. These responsibilities include the development of target recognition systems that can differentiate effectively between non-combatants and combatants or directly participating civilians, careful testing of system reliability before use, exclusion of any systems that fail to meet prescribed performance standards during realistic testing, adequate technological training for those who launch sorties, and appropriate workload management for those individuals charged with intervening, should inappropriate automated or autonomous attack decisions occur.

Conclusion

The fundamental human quality of desiring freedom from harm while simultaneously seeking out the means to project it has constituted one of the core drivers of technological advance since ancient times. Moreover, warfare and the technologies devised to wage war are especially prominent instances in which this quality has had a direct impact. At present, unmanned weapon systems (UWS) are the latest manifestation of this desire to – while protected – project harm, and so it is understandable that governments, in the interests of their states and national security,[90] have

[89] Program on Humanitarian Policy and Conflict Research Manual on International Law - Applicable to Air and Missile Warfare rule 34 and associated Commentary.
[90] Noel Sharkey, 'Saying No! to Lethal Autonomous Targeting' (2010) 9 *Journal of Military Ethics* 369.

been funnelling a substantial proportion of the public fund into the development of increasingly autonomous UWS.[91]

Given the numerous benefits associated with the mobilisation of UWS that have a high degree of operational autonomy, which include force multiplication[92] and minimal risk to human life, recent years have witnessed the growing reliance that contemporary military forces have for these systems.[93] This fact is evidenced by reports that more than 70 countries have now installed UWS (both automated and semi-autonomous) into their military forces,[94] where the United States serves as a particularly prominent example of a state with more than 20,000 UWS.[95]

However, as previously alluded to, the utilisation and deployment of UWS for combat purposes has been debated fiercely both within and among governments. The legality of these systems, especially unmanned combat drones (like those employed by the United States in Pakistan, Somalia, and other states) has long been questioned by scholars,[96] human rights agencies,[97] and United Nations special rapporteurs.[98] It is important to recognise that while the deployment of

[91] See United States Air Force 'UAS Flight Plan 2009-2047' (2009) 41. Available from http://www.scribd.com/doc/17312080/United-States-Air-Force-Unmanned-Aircraft-Systems-Flight-Plan-20092047-Unclassified (accessed 11 November 2017).

[92] 'Autonomous weapons systems act as a force multiplier. That is, fewer war fighters are needed for a given mission, and the efficacy of each war fighter is greater.' Amitia Etzioni and Oren Etzioni, 'Pros and Cons of Autonomous Weapons Systems' (2017) *Military Review* 1.

[93] Peter Singer, *Wired for War: The Robotics Revolution in the 21st Century* (Penguin Reprint edition, 2009); US Department of Defense *Unmanned Systems Integrated Roadmap FY 2013-2038* (2013) 19 https://www.defense.gov/Portals/1/Documents/pubs/DOD-USRM-2013.pdf (accessed 20 October 2017).

[94] See US Department of Defense *Unmanned systems integrated roadmap FY (2013-38)* 6 available at https://www.defense.gov/Portals/1/Documents/pubs/DOD-USRM-2013.pdf (accessed 5 October 2017); US Department of Defence *Dictionary of military and associated terms* (2001) 579; Shashank Joshi & Aaron Stein, 'Emerging Drone Nations' Survival' (2013) 55 *Global Politics and Strategy* 53, 78.

[95] Peter Singer, 'The Predator Comes Home: A Primer on Domestic Drones, Their Huge Business Opportunities, and Their Deep Political, Moral, and Legal Challenges' (8 March 2013) available at http://www.brookings.edu/research/papers/2013/03/08-drones-singer (accessed 10 November 2017); US Department of Defense 'Defense science board, task force report: the role of autonomy in DoD systems' (2012) 78 available at https://fas.org/irp/agency/dod/dsb/autonomy.pdf (accessed 8 November 2017).

[96] See Christof Heyns & Sarah Knuckey, 'The Long-term International Law Implications of Targeted Killing Practices' (2013) 54 *Harvard International Law Journal* 114; Philip Alston, 'The CIA and Targeted Killings Beyond Boarders' (2011) 2 *Harvard National Security Journal* 116.

[97] Human Rights Watch 'Losing Humanity: The Case Against Killer Robots' (2012) available at http://www.hrw.org/reports/2012/11/19/losing-humanity-0 (accessed 9 November 2017); Amnesty International 'United States of America Targeted Killing Policies Violate Right to Life' (2012) http://www.amnesty.org/en/library/info/AMR51/047/2012/en (accessed 9 November 2017).

[98] See UN A/HRC/14/24/Add.6 Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Philip Alston, 28 May 2010; A/68/30532; Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Christof Heyns, 12 August 2013; A/68/389 Report of the Special Rapporteur on the Promotion and

drones as part of a state's military operations is continuously debated among scholars[99], the notion that drones are legal weapons is not currently in doubt.[100] However, in contrast to drones, AWS are objected to on the basis of their perceived illegality,[101] along with the fact that these weapon systems are unethical and immoral.[102] While one might argue that AWS are the natural extension of unmanned combat drones, the distinct feature is that Meaningful Human Control (MHC) is not exercised by an operator over the 'critical functions' of an AWS.

Currently, although the deployment of AWS is not yet a reality,[103] many countries, including North Korea, the United States, and the United Kingdom have developed fully-operational semi-autonomous weapon systems.[104] Perhaps the most famous robotic weapon system (with the capacity for lethal force and the semi-autonomous identification of targets) is Samsung Techwin's machine, currently operational in the 38th Parallel in Korea.[105] This security safeguarding system draws on infrared sensing technology to detect the presence unauthorised personnel and, following this, it can begin to fire ammunition in the identified direction. It should be noted, however, that these systems still rely on MHC.[106]

Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Ben Emmerson, 18 September 2013.

[99] Kenneth Anderson, 'Targeted Killing and Drone Warfare: How We Came to Debate whether there is a Legal Geography of War' in Peter Berkowitz (eds), *Future Challenges in National Security and Law*, Hoover Institution (Stanford University 2011); Christof Heyns, Dapo Akande, Lawrence Hill-Cawthorne and Thompson Chengeta, 'The International Law Framework Regulating the Use of Armed Drones' (2016) 65 (4) *International and Comparative Law Quarterly* 791.

[100] Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Christof Heyns, 12 August 2013, para 13 p.7.

[101] Armin Krishnan, *Killer Robots: Legality and Ethicality of Autonomous Weapons* (Ashgate, 2009); G Marchant et al, 'International Governance of Autonomous Military Robots' (2011) XII *Columbia Science and Technology Law Review* 280.

[102] Patrick Lin et al, *Robot Ethics: The Ethical and Social Implications of Robotics* (MIT Press, 2014); Kenneth Anderson & Matthew Waxman, 'Law and Ethics for Robot Soldiers' (2012) 32 *American University WCL Research* 18; Noel Sharkey, 'The Evitability of Autonomous Robot Warfare' (2012) 94 *International Review of the Red Cross*.

[103] A/HRC/23/47, Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Christof Heyns, p. 8 para 45.

[104] Samsung SGR-A1 (Republic of Korea), MDARS-E (UK), Northrop Grumman X-47B (USA) This is based on data compiled by: Vincent Boulanin, 'Mapping the Development of Autonomy in Weapon Systems: A Primer on Autonomy' (2016) SIPRI Working Paper; Semi-autonomous systems are defined as 'a weapon system that, once activated, is intended to only engage individual targets or specific target groups that have been selected by a human operator.'- US Department of Defense *Autonomy in Weapon Systems, Directive 3000.09* (2012) 14 available at http://www.dtic.mil/whs/directives/corres/pdf/300009p.pdf (accessed 3 November 2017).

[105] Jonas Ebbesson et al, *International Law and Changing Perceptions of Security: Liber Amicorum Said Mahmoudi* (Brill, 2014) 167.

[106] Jean Kumagai, 'A Robotic Sentry for Korea's Demilitarized Zone' (2007) 44 *Institute of Electrical and Electronics Engineers Spectrum* 2.

Another example is Israel's autonomous weapon system, the 'Harpy', the purpose of which is to identify, attack, and eradicate radar emitters.[107] In a similar vein, the United Kingdom is currently designing 'Taranis', a fight-jet-inspired combat drone which can independently collect environmental data, locate targets, and engage in defensive action.[108] At present, the implementation of lethal force cannot be initiated by the system itself; rather, Taranis mission command must implement these 'critical functions'. Yet another high-technology weapon system is being developed by the US Navy (Northrop Grumman Company as contractor), the 'X-47B' drone. The system has the capacity to facilitate launch, landing, and navigation in an operator-independent manner, and it can also discharge lethal force autonomously under predetermined circumstances.[109] Perhaps the critical point to emphasise from an overview of the contemporary technological landscape is that states are presently developing increasingly autonomous UWS, many of which represent major strides forward towards AWS.

[107] UC Jha, *Killer Robots: Lethal Autonomous Weapon Systems Legal, Ethical and Moral Challenges* (VIJ Books, 2017) 36.
[108] UC Jha, *Killer Robots: Lethal Autonomous Weapon Systems Legal, Ethical and Moral Challenges* (VIJ Books, 2017) 41.
[109] See Northrop Grumman, 'X-47B UCAS' At: http://www.northropgrumman.com/Capabilities/x47bucas/Pages/default.aspx (accessed 17 October 2017).

Chapter 2 - The Compliance of Autonomous Systems with International Humanitarian Law

Introduction

International dialogue on the use of Autonomous Weapon Systems (AWS) has, until now, concentrated predominantly on the humanitarian aspect. Discussions have centred on International Humanitarian Law (IHL). As such, researchers have long debated the ability of AWS to adhere to the IHL principles of an attack being discriminate, militarily necessary and proportionate. Many hold that the use of AWS is only acceptable if the systems are proven to adhere to these fundamental principles of IHL.

There are a number of conflicting opinions on whether AWS are able to adhere to IHL, with three key schools of thought. The first group hold that the technology is so new and untested that it is impossible to know whether or not AWS can comply with IHL.[110] This group states that international action which regulates autonomous weapons would be ill-advised.[111] As such, they do not agree with a complete ban on AWS, believing that such an embargo could create a 'risk of failing to develop forms of automation that might make the use of force more precise and less harmful to civilians caught near it'.[112] Faced with such a restriction, some believe that state actors involved in AWS development 'should not unnecessarily constrain themselves in advance to a set of normative commitments given the vast uncertainties about the technology and future security environment.'[113] It would appear that many academics within the field remain undecided on the matter, and are hesitant to draw any conclusions until the technology is available. Such hesitation, however, is concerning, as retrospective regulation of weaponry is difficult and, in the case of

[110] Geoffrey Corn, 'Autonomous Weapons Systems: Managing the Inevitability of Taking the Man Out of the Loop' in Nehal Bhuta, Susanne Beck, Robin Geiβ, Hin Liu, & Claus Kreβ (eds), *Autonomous Weapons Systems: Law, Ethics, Policy* (Cambridge University Press, 2016) 242; Kjolv Egeland, 'Lethal Autonomous Weapon Systems under International Humanitarian Law' (2016) 85 *Nordic Journal of International Law* 117.
[111] Kenneth Anderson and Matthew C Waxman, 'Law and Ethics for Autonomous Weapon Systems: Why a Ban Won't Work and How the Laws of War Can' (Hoover Institution, 9 April 2013) 3.
[112] Kenneth Anderson and Matthew Waxman, 'Law and Ethics for Autonomous Weapon Systems: Why a Ban Won't Work and How the Laws of War Can' (Hoover Institution, 9 April 2013) 1.
[113] Kenneth Anderson & Matthew Waxman, 'Law and Ethics for Robot Soldiers' (2012) 32 *American University WCL Research Paper* 18.

AWS, could potentially be ineffective.[114] Even more concerningly, such hesitation could be strategic, allowing the technology to enter development uncontested.

A second group of commentators believe that AWS may be more effective than human fighters in complying with IHL. This view stems from the fact that AWS are emotionally unbiased systems, unaffected by anger, frustration, shock, or a desire for revenge.[115] Unless deliberately pre-programmed by their human operators to do so, an AWS will never knowingly commit a war crime.[116] For this school of thought, the key argument is that AWS will not only assist soldiers on the ground, but also protect innocent civilians from victimisation.[117]

The final major school of thought on AWS holds that such systems will never have the situational awareness required to interpret the full context of an attack. Such awareness is, they argue, vital on the battlefield, and something which AWS will never have. According to this group, without this deeper understanding, AWS will never be fully compliant with IHL.[118]

In this chapter, I present a number of arguments that combine to conclude that AWS cannot be generalised when assessing their compliance with IHL. Each AWS has its own individual level of autonomy.[119] This chapter will consider, in particular, systems that are highly autonomous, even

[114] See A/HRC/23/47, Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Christof Heyns, 9 April 2013.
[115] GE Marchant et al, 'International Governance of Autonomous Military Robots' (2011) XII *The Columbia Science and Technology Law Review* 280; Jai Galliott, *Military Robots: Mapping the Moral Landscape* (Routledge, 2015) 270; Peter Margulies, 'Making Autonomous Weapons Accountable: Command Responsibility for Computer-Guided Lethal Force in Armed Conflicts' in Jens David Ohlin (eds), *Research Handbook on Remote Warfare* (Edward Elgar, 2016) 442.
[116] See A/HRC/23/47, Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Christof Heyns, 9 April 2013.
[117] Ronald Arkin, 'Lethal Autonomous Systems and the Plight of the Non-combatant' in Ryan Kiggins (eds), *The Political Economy of Robots International Political Economy Series* (Palgrave Macmillan, 2018) 9.
[118] Jarna Petman, 'Autonomous Weapons Systems and International Humanitarian Law: Out of the Loop?' (2017) Research Report Ministry for Foreign Affairs of Finland; Tetyana Krupiy, 'Of Souls, Spirits and Ghosts: Transposing the Application of the Rules of Targeting to Lethal Autonomous Robots' (2016) 16(1) *Melbourne Journal of International Law* 145; Nicholas Mull, 'The Roboticization of Warfare with Lethal Autonomous Weapon Systems (Laws): Mandate of Humanity or Threat to It?' (2017) *Houston Journal of International Law* 63.
[119] William Marra et al, 'Understanding the Loop: Regulating the Next Generation of War Machines' (2013) 36 *Harvard Journal of Law and Public Policy* 1155; See also US Department of Defense Unmanned Systems Integrated Road Map FY2011-2036 (2011) 44. Available at <http://www.acq.osd.mil/sts/docs/Unmanned%20Systems%20Integrated%20Roadmap%20FY2011-2036.pdf> (accessed 15 August 2018).

unpredictable, and those that, once activated, have no 'Meaningful Human Control'. For highly autonomous platforms, or those which are not subject to 'Meaningful Human Control', are unable to perform proportionate attacks and may be insufficient to differentiate civilians, protected persons and objects.[120] This is caused, in particular, by the shifting context of the battle space, the unpredictability of civilians' status and the platforms' own technological restrictions.[121]

Even when operated in zones that are solely occupied by adversaries, fully autonomous systems are still at risk of breaking IHL, providing insufficient protections to injured and, thus, *hors de combat* adversaries and those who choose to surrender.[122] I do not agree that robots are more likely to comply with IHL. Even in a scenario whereby robots were indeed more compliant, other factors would need to be considered. Affording a robot, the power to take human life could contravene basic human rights such as the right to life, the right to bodily integrity, the right to dignity as they are currently understood, even when considering the context of armed conflict and accurate, legal targeting.[123] In terms of the principle of precaution, it could well be feasible for AWS to exercise such control, with systems waiting until they come under fire before concluding that an adversary is indeed engaged in combat.[124] Without human oversight, precaution, as with distinction and proportionality, cannot be guaranteed.[125] Should humans be removed from the operational chain upon system activation, it is likely that these rules would be compromised. For highly autonomous and, as such, unpredictable platforms, or those which are not subject to 'Meaningful Human Control', their post-activation actions may violate IHL.

This chapter will examine the potential for conflicts between Autonomous Weapons Systems and International Humanitarian Law and examine the ways in which these may be addressed. The ways

[120] On IHL rules see in general Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law* (Cambridge University Press, 2005) vols 1 and 2.
[121] Geneva Academy of International Humanitarian Law 'Autonomous Weapon Systems under International Law' (2014) *Academy Briefing Number 8* 24.
[122] Andrew Clapham & Paola Gaeta, *The Oxford Handbook of International Law in Armed Conflict* (Oxford University Press, 2014) 308.
[123] Gerd Oberleitner, *Human Rights in Armed Conflict* (Cambridge University Press, 2015) 1.
[124] A/HRC/23/47, Report of the UN Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Christof Heyns, para 69.
[125] Peter Asaro, 'On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-Making' (2012) 94 *International Review of the Red Cross* 693, 696; Geneva Academy of International Humanitarian Law 'Autonomous Weapon Systems under International Law' (2014) *Academy Briefing No 8*, 5.

in which IHL works and how it is applicable to AWS will be examined, looking at the key concept of distinction.

Can AWS Be Deployed in Compliance with the Principle of Distinction?

Distinction, is considered to be 'the most significant battlefield concept'[126] because *ratio legis* of this rule is referred to protect civilians, *hors de combat*, essentially those who are not taking part in hostilities and presents the first and seventh rules of the International Committee of the Red Cross (ICRC) Customary IHL Study. The customary nature of distinction is not in question.[127] Further, Article 48 of Additional Protocol I is considered a Basic Rule[128] which indicates that no reservation is permitted, and no state seeks to involve in a reservation[129] also described by the Red Cross as a 'foundation on which the codification of the laws and customs of war rests.'[130] Otherwise put, distinction is one of the fundamental concepts 'constituting the fabric of humanitarian law.'[131] According to Solis, distinction is 'embedded in virtually all aspects [of

[126] Gary Solis, *The Law of Armed Conflict: International Humanitarian Law in War* (Cambridge University Press, 2010) 251.
[127] See for instance Eritrea-Ethiopia Claims Commission, Partial Award, Western Front, Aerial Bombardment and Related Claims, Eritrea's Claims 1, 3, 5, 9-13, 14, 21, 25 and 26 (19 December 2005), Report of International Arbitration Awards, vol XXVI, 291-349.
[128] Article 48 'In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.' Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.
[129] See for example statements of the UK and Mexico in the Diplomatic Conference for the Adoption of the Additional Protocols to the Geneva Conventions of 1949.
[130] Yves Sandoz, Christophe Swinarski and Bruno Zimmerman (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August* (Martinus Nijhoff, 1987) para.598.
[131] *Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)* [1996] ICJ Rep 1996, 257.

IHL].'[132] Additional Protocol II also appears to tackle the matter of distinction, although somewhat timidly.[133] It is, however, already woven into the fabric non-international conflict.[134]

Persons

In line with the bifurcated nature of the distinction principle, AWS will need to categorise persons either as combatants, who may be directly attacked; or as civilians, or other protected persons, who must be spared and protected from direct attack.

Active Combatants

The General Position

Combatants are generally members of the conventional armed forces who have the right to participate directly in hostilities,[135] or members of 'other militias and…volunteer corps' who meet certain conditions,[136] and who will be engaged during (tactical-level combat) TLC. These persons may be detectable to (automatic target recognition) ATR via their distinctive uniform and insignia,[137] which Parties to armed conflict are obliged to wear to remain 'recognizable at a distance'.[138] The underlying aim is to make combatants distinguishable from the civilian population, for the latter's protection,[139] but the flipside is to make them amenable to machine

[132] Gary Solis, *The Law of Armed Conflict: International Humanitarian Law in War* (Cambridge University Press, 2010) 254.
[133] See Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (adopted on 8 June 1977, entered into force 7 December 1978) 1125 UNTS 609 art 13(1) and (2). Additional Protocol II (draft)-Article 24(1) of the draft Additional Protocol II submitted by the ICRC to the CDDH provided: 'In order to ensure respect for the civilian population, the parties to the conflict shall confine their operations to the destruction or weakening of the military resources of the adversary.' CDDH, Official Records, Vol. I, Part Three, Draft Additional Protocols, June 1973, p. 37. This proposal was amended and adopted by consensus in Committee III of the CDDH. CDDH, Official Records, Vol. XV, CDDH/215/Rev.1, 3 February–18 April 1975, 288, § 113. The approved text provided: 'In order to ensure respect and protection for the civilian population … the Parties to the conflict … shall direct their operations only against military objectives.' CDDH, Official Records, Vol. XV, CDDH/215/Rev.1, 3 February–18 April 1975, 319. Eventually, however, it was deleted in the plenary, because it failed to obtain the necessary two-thirds majority (36 in favour, 19 against and 36 abstentions). CDDH, Official Records, Vol. VII, CDDH/SR.52, 6 June 1977, 135, § 78.
[134] Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law – Volume I: Rules* (Cambridge University Press, 2005) 5, 8.
[135] Article 43(2), AP I; *AMW Manual Commentary*, Rule 10(b)(i).
[136] Article 1, Annex to Convention (IV) Respecting the Laws and Customs of War on Land: Regulations Concerning the Laws and Customs of War on Land (adopted 18 October 1907, entered into force 26 January 1910) 36 Stat. 2227 TS 539; Article 4A(2), Geneva Convention (III) Relative to the Treatment of Prisoners of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 135.
[137] See 'Camopedia: The Camouflage Encyclopedia' <http://camopedia.org/index.php?title=Main_Page> accessed 11 December 2020.
[138] Article 1(2), Hague Regulations; Article 4A(2)(b), GC III.
[139] Article 44(3), AP I; CIHL, Rule 106; *AP I Commentary*, 1578.

perception for lethal targeting.[140] That said, reliance on uniform and insignia alone may lead to distinction failure as combatants may become *hors de combat*; civilians may take the clothing of deceased soldiers and unwittingly put themselves in the crosshairs of a AWS; or, the enemy may utilise adversarial examples to direct attacking forces towards civilians, in a propaganda war. All three risks counsel in favour of broader criteria and/or multisensory phenomenologies, for a more robust verification of combatant status. One solution may be to combine uniform and insignia with the recognition of specific arms and equipment used exclusively by the enemy.[141] The fact that combatants are legally required to carry their arms openly[142] as a second condition of distinction supports this. A more effective approach may be to detect the metallic footprint and the distinctive behaviour and movements, which are a product of military training.[143] Together with uniform and insignia detection this provides a robust three-part criteria, namely, the combination of a) uniform and insignia, b) metallic footprint, and c) the distinctive behaviour and movements, which are a product of military training which may also be combined with specific arms recognition when it is desirable to attain a higher confidence threshold. Along with the legal status of privileged (enemy) combatants, we may expect to see a relatively firm basis for status-based targeting in international armed conflict. Namely, once combatant status is established there are no legal grey areas: active combatants may be attacked based solely on their status, irrespective of the extent of their involvement in hostilities.[144] To be sure, while a small subset of IHL scholars argues for a so-called 'duty to capture',[145] the overwhelming academic opinion is for status-based targeting;[146] as is the evident legal authority.[147] This clearly supports administrability by precluding the need for a AWS to undertake any metacognitive conduct-based evaluation, or individualised threat assessment.

---

[140] Christopher M. Ford, 'Autonomous Weapons and International Law' (2017) 69 South Carolina Law Review 413, 436.
[141] Rao Komar, 'How to Digitally Verify Combatant Affiliation in Middle East Conflicts', *Bellingcat* (9 July 2018) <https://www.bellingcat.com/resources/how-tos/2018/07/09/digitally-verify-middle-east-conflicts/> accessed 11 December 2020.
[142] Article 1(3), Hague Regulations; Article 44(3), AP I; CIHL, Rule 106.
[143] William H. Boothby, 'Autonomous Attack – Opportunity or Spectre?' in Terry D. Gill (ed.), *Yearbook of International Humanitarian Law 2013*, Vol. 16 (TMC Asser Press, 2015), 79.
[144] *Prosecutor* v. *Kordić & Čerkez* (ICTY Appeals Judgment) IT-95-14/2-A (17 December 2004), 51.
[145] Ryan Goodman, 'The Power to Kill or Capture Enemy Combatants' (2013) 24 The European Journal of International Law 819
[146] Laurie R. Blank et al., 'Belligerent Targeting and the Invalidity of a Least Harmful Means Rule' (2013) 89 International Law Studies 536
[147] *Prosecutor* v. *Kordić & Čerkez* (Appeals), 51.

However, AP I blurs the 'combatant' category by including other persons who are less amenable to ATR, such as paramilitary personnel or armed police officers.[148] That said, the Party integrating such personnel into its armed forces must notify the other Parties to the conflict, to avoid confusion.[149] This will enable the latter to update the ATR of their AWS, to recognise the relevant uniform and insignia,[150] and the specific arms being used by the paramilitary/police agency.

Even more challenging is the inclusion of guerrilla fighters wearing no uniform or distinguishing sign, and with relaxed rules on the open carriage of their weapons.[151]

This is a significant drawback for an AWS-deploying Party as it undermines the objective dimension of status-based targeting, which is where machines are likely to excel. However, not all States that are expected to field AWS are Party to AP I, or bound by any (debatable) equivalent rule in customary law.[152] Persistent objectors include the US[153] and Israel,[154] who specifically admonish Article 44(3) and do not recognise it as having customary status,[155] but instead use the traditional categories of combatant found in Article 4A, GC III. Other States that are bound by Article 44(3) have generally expressed three limiting factors, which further narrow the exception and minimise its negative impact on the utilisation of AWS.[156] In any event, they can always restrict their AWS deployments to traditional battlefields, where uniformed combatants are the norm, and which will be relatively more amenable to ATR.[157]

---

[148] Article 43(3), AP I; *AMW Manual Commentary*, Rule 10(b)(i), 3.
[149] Article 43(3), AP I; *AMW Manual Commentary*, Rule 10(b)(i), 3.
[150] CIHL Customary International Humanitarian Law Study, Rule 4.
[151] Article 44(3), AP I.
[152] CIHL, Rule 106.
[153] See also the authoritative position of the US on AP I in 'Memorandum for Assistant General Counsel (International), Office of the Secretary of Defense, 1977 Protocols Additional to the Geneva Conventions: Customary International Law Implications' (8 May 1986)
[154] See 'Israel, Statement at the Diplomatic Conference Leading to the Adoption of the Additional Protocols', *Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts, Vol. VI* (Federal Political Department, 1978), CDDH/SR 40, 17.
[155] US Department of Defense, *Law of War Manual* (Office of General Counsel, DoD, 2015, December 2016 Update) § 4.6.1.2; Ted L. Stein, 'The Approach of the Different Drummer: The Principle of the Persistent Objector in International Law' (1985) 26 Harvard International Law Journal 457.
[156] The *Official Records of the Diplomatic Conference* (n 95), CDDH/SR 40-41.
[157] Geoffrey S. Corn, 'Thinking the Unthinkable: Has the Time Come to Offer Combatant Immunity to Non-State Actors?' (2011) 22 Stanford Law & Policy Review 253.

Yet, even traditional combatants will not always be a guarantee of adequate distinction. For example, adversarial static may be embedded in military uniform to spoof a AWS into perceiving civilian clothing; this may amount to no more than a lawful ruse of war if the spoofing Party merely diverts the AWS away from itself to avoid coming under attack.[158] Indeed, such a move may even be comparable (albeit inversely) to the use of chaff and flares, which has long been practiced by military pilots to divert radar-guided and infrared-guided missiles.[159] On the other hand, if the adversarial static imitates *enemy* uniform and insignia (or flags/emblems) to shield, favour, protect or impede military operations, this would very likely be prohibited under Article 39(2), AP I.[160] Furthermore, if such misuse extends to static-generated uniforms, signs or emblems of the UN or neutral/non-Party States (or civilian clothing patterns) in order to feign protected status; and if this leads to the killing, injuring or capture of AWS-deploying personnel, it will be deemed to be a perfidy under Article 37(1).[161]

In this regard, Sassóli poses the question as to whether a machine can be led to believe that the person or object before it has protected status, or whether it is possible to invite the confidence of an AWS – two vital elements of perfidy.[162] Arguably, such anthropomorphic terms cannot directly apply to an AWS. On the other hand, any manipulation of visual data by an adverse Party that causes an AWS to hold fire may, by extension, invite the confidence of human combatants who rely on ATR assessments and/or are led by the actions of their machine 'partners'. This may possibly lead those human combatants to believe that the person or object before them enjoys protected status. If such a scenario played out and adverse forces killed, injured or captured attacking forces as a result, perfidy would be very likely to be established.

There are limitations to this prohibition: property damage (including damage to the AWS unit) is not covered by perfidy,[163] even if this does degrade combat capability. However, this may not

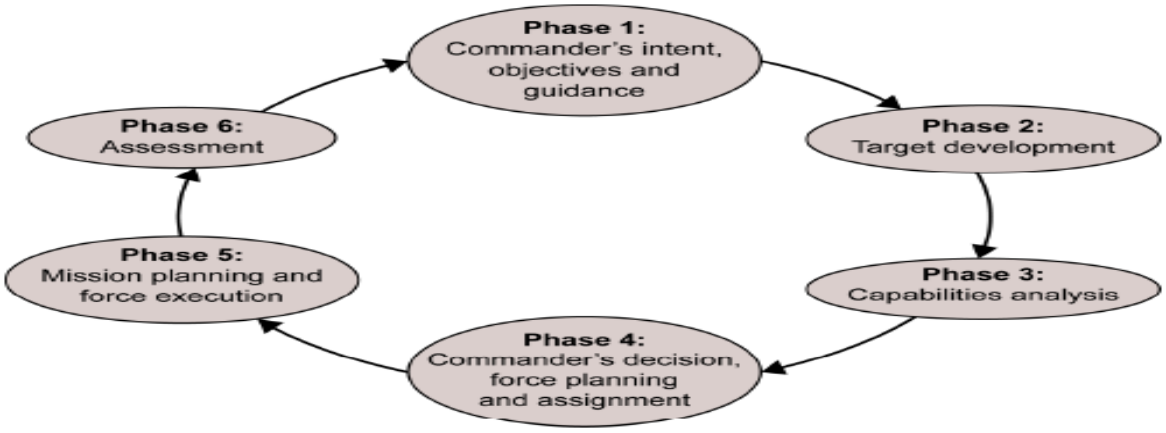
[158] Article 37(2), AP I; *AMW Manual*, Rule 113; CIHL, Rule 57.
[159] See the examples of (especially US) State practice under CIHL, Rule 57 <https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule57> accessed 11 December 2020.
[160] Article 39(2), AP I; *AMW Manual*, Rule 112(c); CIHL, Rule 62.
[161] Article 37(1), AP I; *AMW Manual*, Rule 111(a)-(b); CIHL, Rule 65.
[162] Marco Sassóli, 'Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified' (2014) 90 International Law Studies 328.
[163] *AMW Manual Commentary*, Rule 111(a), 7.

matter in the case of Article 39(2), which is drafted broadly enough ('impede military operations') to catch property damage or any other degradation to combat capability. The legal difference therefore hinges on whether the adversarial examples centre around enemy uniform and insignia (or flags/emblems); or whether they imitate civilian clothing, or the uniforms, signs or emblems of neutral/non-Party States.

It should be noted that resolving the problem of adversarial examples in uniform is not solely dependent on a legal solution. A more pragmatic approach may be for intelligence analysts to determine – most likely during Phase 2 of the deliberate targeting cycle – how adversarial examples are being utilised by the enemy. Thereon, systems may be trained to recognise specific examples and even specific kinds of adversarial patterns in enemy uniform, before being deployed at Phase 5.[164]

Civilians and Other Protected Persons

In contradistinction to the above, Article 51(2) prohibits making civilians the object of attack,[165] as well as acts or threats of violence for the primary purpose of terrorising the civilian population.[166] Paragraph (6) prohibits attacks against civilians by way of reprisal,[167] and this is of peremptory importance,[168] given how easily reprisals have in the past been invoked as a pretext



[164] The NATO Joint Targeting Cycle. Source: AJP-3.9, 2-2.
[165] Article 51(2), AP I; *AMW Manual*, Rule 11; CIHL, Rule 1.
[166] Article 51(2), AP I; *AMW Manual*, Rule 18; CIHL, Rule 2.
[167] Article 51(6), AP I. See also CIHL, Rule 145.
[168] *AP I Commentary*, 1984.

for indiscriminate warfare. Arguably, the nature and wording of these prohibitions renders compliance relatively simple: a matter of *ex ante* programming and appropriate deployment, which should pose no difficulty for commanders acting in good faith.[169]

The issue differs when considering the general civilian protection afforded in Paragraph (1),[170] Article 48[171] and in customary law.[172] None of these presume deliberate targeting on the part of human participants, and all of them may be violated when there is distinction failure on the part of the machine, if this would not occur in a counterfactual manned targeting scenario.[173] Yet, even here a AWS is – at least in more traditional battlefield contexts – arguably capable of respecting civilian status by recognising 'any non-positively identified person' as a civilian.[174] This kind of programming is consistent with the negative definition of civilian in Article 50(1), AP I,[175] and it would entail a technical prohibition on targeting any person not satisfying the three-/four-part criteria discussed above. Thus, far from being vague and non-executable in machine code, it simply requires programming the inverse of the status-based criteria.[176]

[169] Michael N. Schmitt, 'Autonomous Weapons Systems and International Law', *LENS Conference 2016: Autonomous Weapons in the Age of Hybrid War* (27 February 2016) <https://www.youtube.com/watch?v=b5mz7Y2FmU4> accessed 11 December 2020.
[170] Article 51(1), AP I.
[171] Article 48, AP I.
[172] CIHL, Rules 1 and 6.
[173] *AMW Manual Commentary*, Rule 39, 4.
[174] Michael N. Schmitt, 'Autonomous Weapons Systems and International Law', *LENS Conference 2016: Autonomous Weapons in the Age of Hybrid War* (27 February 2016) <https://www.youtube.com/watch?v=b5mz7Y2FmU4> accessed 11 December 2020.
[175] Article 50(1), AP I; *AMW Manual Commentary*, Rule 11, 6; CIHL, Rule 5; *Prosecutor* v. *Blaškić* (ICTY Trial Judgment) IT-95-14-T (3 March 2000), 180.
[176] Noel E. Sharkey, 'The Evitability of Autonomous Robot Warfare' (2012) 94 International Review of the Red Cross 787, 789

Other persons who must be both respected and protected include medical,[177] religious[178] and humanitarian relief personnel,[179] amongst others.[180] On the one hand, these specific categories of persons may require no further programming efforts than those that will be afforded to civilians, as these persons will also satisfy the inverse of the status-based criteria for combatants. This is helpfully reinforced by the restriction of medical personnel to 'light individual weapons'[181] in AP I[182] and in the *2016 GC I Commentary*,[183] to avoid the perception that they are equipped to commit (outside their humanitarian duties) acts harmful to the enemy. Namely, as permissible and restricted arms are all amenable to object recognition, these rules will potentially support respect for medical personnel by AWS-deploying forces.

On the other hand, respect may be bolstered by programming additional (positive) forbidding criteria when these persons bear machine-perceptible signs. Specifically, medical and religious personnel are required to wear a water-resistant armlet bearing the emblem of the Red Cross or Red Crescent, to denote protected status to attacking forces.[184] Moreover, when carrying out their duties in a battle area, these persons shall – as far as possible – wear headgear and clothing that also bears the distinctive emblem,[185] and they may (should) use materials that make the emblem recognisable by technical means of detection.[186] These should further increase the likelihood of reliable machine perception and the application of forbidding criteria by a AWS.

---

[177] Articles 24 and 25, Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 31 (hereafter, GC I); Article 36, Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 85 (hereafter, GC II); Article 20, Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 287 (hereafter, GC IV); Article 15(1), AP I; *AMW Manual*, Rule 71; CIHL Rule 25.

[178] Article 24, GC I; Article 36, GC II; Article 15(5), AP I; *AMW Manual*, Rule 71; CIHL Rule 27.

[179] Article 71(2), AP I; Article 7(2), Convention on the Safety of United Nations and Associated Personnel (adopted 9 December 1994, entered into force 15 January 1999) 2051 UNTS 363; *AMW Manual*, Rule 102(a); CIHL, Rule 31.

[180] Articles 26 and 27, GC I.

[181] Heather Brandon, 'Joint Series: Restricting Medical Personnel, Units, and Transports to 'Light Individual Weapons'', *Intercross Blog* (16 February 2017) <http://intercrossblog.icrc.org/blog/joint-series-restricting-medical-personnel-units-and-transports-to-light-individual-weapons> accessed 17 December 2020.

[182] Article 13(2)(a), AP I; *AMW Manual*, Rule 74(c)(i).

[183] Knut Dörmann et al. (eds.), *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field* (CUP, 2016), 1864 and 1874.

[184] Articles 38-41, GC I; Articles 41-42, GC II; Article 4 and 5, Annex I to Protocol I Additional to the Geneva Conventions of 1949: Regulations Concerning Identification (as amended on 30 November 1993, entered into force 1 March 1994) (hereafter, Amended Annex I); *AMW Manual*, Rule 72(a); CIHL, Rule 30.

[185] Article 5(4), Amended Annex I.

[186] Article 5(3), Amended Annex I; *AMW Manual Commentary*, Rule 72(b), 2.

So far, there appears to be a relatively clear textual basis for distinction between categories of persons, which AWS may be expected to satisfy in at least some circumstances. However, in contemporary conflicts sub-categories often appear, which complicate the distinction task.

Civilians Not Protected from Direct Attack

In particular, civilians may take a direct part in hostilities (DPH) and, *for such time* that they do, they become targetable.[187] This temporal element complicates matters because to be liable to attack, a civilian must act on a 'spontaneous, sporadic or unorganised basis'[188] and must, in the view of the ICRC, cumulatively meet its *threshold of harm* with *direct causation* and a *belligerent nexus*.[189] Moreover, measures taken to prepare for a specific act of DPH, as well as deployment to and from the location of that act, also qualify as DPH.[190] On the other hand, the ICRC considers there to be a 'revolving door', whereby suspension of civilian protection lasts only as long as the person engages in DPH, even if there are persistently recurrent cycles.[191] While this legal view is often disputed,[192] it is generally acknowledged that the factual circumstances giving rise to DPH in the first instance are not always objectively discernible.[193]

This creates a conduct-based targeting challenge that will be very difficult for near-term AWS to meet. Specifically, ATR systems will find it very difficult to recognise offensive behaviour from

[187] Article 51(3), AP I; *AMW Manual*, Rule 28; CIHL Rule 6.
[188] International Committee of the Red Cross (ICRC), *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law* (ICRC, 2009), 34.
[189] International Committee of the Red Cross (ICRC), *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law* (ICRC, 2009), 64.
[190] International Committee of the Red Cross (ICRC), *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law* (ICRC, 2009), 68.
[191] International Committee of the Red Cross (ICRC), *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law* (ICRC, 2009), 73.
[192] William H. Boothby, 'Direct Participation in Hostilities – A Discussion of the ICRC Interpretive Guidance' (2010) 1 International Humanitarian Legal Studies 143, 162; Michael N. Schmitt, 'The Interpretive Guidance on the Notion of Direct Participation in Hostilities' (2010) 1 Harvard National Security Journal 5, 36 (arguing that 'for such time' should extend "as far before and after a hostile action as a causal connection existed"); *US DoD Manual*, §5.8.4.1.
[193] Michael N. Schmitt and Eric W. Widmar, 'On Target: Precision and Balance in the Contemporary Law of Targeting', (2014) 7 Journal of National Security Law & Policy 379, 390 ("The status of an individual can sometimes be unclear…consider…civilians sitting on a hillside overlooking a commonly used helicopter landing zone. Without additional intelligence indicating they are being used as an early warning system…IHL requires them to be treated as civilians and protected from attack").

a civilian, with no other tangible cues.[194] On the other hand, three potential solutions have been suggested. First, Henderson, Keane and Liddy argue that some DPH indicators currently applied by human decision-makers are relatively tangible, and may be programmed into a AWS.[195] These include whether an individual is openly armed; his proximity to the fighting and/or other military equipment; and the direction and manner of his movement.[196] So long as each characteristic is appropriately weighted, it is conceivable that a combination of such criteria pointing in the same direction might be a strong indicator of a civilian undertaking DPH. However, this approach seems plausible only in a limited range of circumstances, with much scope for erroneous targeting. Namely, it ignores the near-infinite combinations of relevant cues, the metacognitive approach of human soldiers in situations of uncertainty and their reliance on "gut feeling"[197] versus the deterministic response of a robot.

Second, Ford considers a narrow deployment approach, focusing on the common insurgency practice of emplacing an improvised explosive device along a road. The author argues that this is both amenable to machine perception and it potentially justifies lethal attack by an AWS, in a way compatible with the ICRC's *Interpretive Guidance*.[198] However, this kind of deployment may also be subject to targeting error. For example, an AWS may detect a person with explosive chemical signatures on a construction site, and open fire on civilians undertaking innocuous commercial activity; though there are also control mechanisms to mitigate this risk.

Finally, perhaps the most commonly-cited approach is Arkin's conservative use of lethal force concept.[199] This argues that robots do not necessarily have a self-preservation instinct, thus can be

[194] Markus Wagner, 'The Dehumanization of International Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapon Systems' (2014) 47 Vanderbilt Journal of Transnational Law 1371, 1392-93
[195] Ian S. Henderson, Patrick Keane and Josh Liddy, 'Remote and Autonomous Warfare Systems: Precautions in Attack and Individual Accountability' in Jens David Ohlin (ed.), *Research Handbook on Remote Warfare* (Edward Elgar, 2017), 346-47.
[196] Ian S. Henderson, Patrick Keane and Josh Liddy, 'Remote and Autonomous Warfare Systems: Precautions in Attack and Individual Accountability' in Jens David Ohlin (ed.), *Research Handbook on Remote Warfare* (Edward Elgar, 2017), 347.
[197] Robin Geiss, *The International Law Dimension of Autonomous Weapons Systems* (Friedrich Ebert Stiftung Study, October 2015), 14
[198] Christopher M. Ford, 'Autonomous Weapons and International Law' (2017) 69 South Carolina Law Review 438.
[199] Ronald C. Arkin, *Governing Lethal Behaviour in Autonomous Robotics* (Chapman & Hall/CRC, 2009), 46.

programmed to hold fire on all civilians until fired upon.[200] Arguably, opening fire on a AWS goes beyond mere hostile intent and may be regarded as *prima facie* evidence of a specific hostile act, which is the very essence of DPH.[201] Moreover, with the use of optical/acoustic detection systems, gunfire is easily recognisable by a robot and should legally permit a defensive lethal response. However, even this approach is problematic. Gunfire is merely target indication, which in most cases will require a tipping and cueing of sensors and further (automatic or controlled) processing before it can progress to full target identification. Thus, relying on gunfire alone may lead to numerous other problems, including:

- The risk of shoot and scoot, where insurgents open fire from areas of civilian concentration, before fleeing to confuse the adversary.[202] This may become a common baiting tactic if AWS are deployed in urban areas or equipped with indirect fires,[203] and it may lead them to return fire into civilian areas, even though a metacognitive human may have had cause to hesitate and reassess.

- The risk that the insurgent is using a human shield, and the likelihood that an AWS will return fire and kill the latter. While the legal status of human shields is controversial,[204] there is near-consensus that *involuntary* human shields retain their protected status.[205] In which case, precautions in attack must be taken, and any expected harm to them must be fully factored into the proportionality assessment.

- In the most chaotic situations, there is the broader risk of civilians being caught in the cross-fire, as well as fratricide.[206]

Consequently, while narrow conditions may exist where civilians taking DPH are amenable to autonomous attack, the risk of unforeseen circumstances, elusive behaviour and consequent

[200] Michael N. Schmitt and Jeffrey S. Thurnher, 'Out of the Loop: Autonomous Weapon Systems and the Law of Armed Conflict' (2013) 4 Harvard National Security Journal 231, 264.
[201] see NATO Military Committee, *NATO Rules of Engagement*, MC 362/1 (NATO HQ, 30 June 2003), 3-5.
[202] Michael N. Schmitt, 'The Principle of Distinction and Weapon Systems on the Contemporary Battlefield' (2008) 7 Connections 46, 54.
[203] Colonel Richard Jackson, 'Autonomous Weaponry and Armed Conflict', *ASIL Panel Discussion* (10 April 2014) <https://www.youtube.com/watch?v=duq3DtFJtWg> accessed 10 December 2020.
[204] Michael N. Schmitt, 'Human Shields in International Humanitarian Law' (2009) 47 Columbia Journal of Transnational Law 292.
[205] Ian Henderson, *The Contemporary Law of Targeting: Military Objectives, Proportionality and Precautions in Attack under Additional Protocol I* (Martinus Nijhoff, 2009), 215.
[206] Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (Norton, 2018), 253-55.

distinction failure is arguably too great to give AWS target engagement authority in a DPH setting. Thus, near-term AWS deployments will be better-suited to traditional battlefields, where enemy combatants offer a clearer basis for distinction.

Persons Hors de Combat

Yet, even in such battlefields, there may remain the problem of systems not recognising when combatants become persons *hors de combat*, and thus protected from direct attack.[207] This may occur in one of three ways: a) capture by friendly forces, b) clearly expressing an intention to surrender, or c) incapacitation, hence an inability to defend oneself.[208] The first of these is not relevant to AWS, as captured personnel are under the control of the AWS-deploying side.[209] The second may be simple or difficult, depending on context and circumstances. For example, in demilitarised zones some basic surrender recognition capabilities currently exist,[210] which may be complemented by more recent developments in deep learning for emotion-reading. In active combat situations, there are a number of other potential (albeit imperfect) solutions,[211] the most robust being a restriction of AWS deployments to particular operational environments; for example, combat between armoured vehicles or submarines, where established conventions on surrender are amenable to machine perception.[212] In the case of anti-personnel targeting, there is also the fact that persons *hors de combat* – be that via surrender or incapacitation – will clearly cease any military-style behaviour and movements, and this may negate the three-/four-part criteria for detecting active combatant status.[213]

However, in more difficult surrender contexts, as well as incapacitation that is not amenable to machine perception, the technical challenges will bring into play some important legal questions. The wording of Article 41(1), AP I, is particularly important here, where it prohibits the targeting of anyone "who is recognized or who, in the circumstances, should be recognized to be *hors de*

[207] Article 41(1), AP I; *AMW Manual*, Rule 15(b); CIHL, Rule 47.
[208] Article 41(2), AP I; *AMW Manual*, Rule 15(b); CIHL, Rule 47.
[209] *AMW Manual Commentary*, Rule 15(b), 3.
[210] See 'Samsung Techwin SGR-A1 Sentry Guard Robot', *GlobalSecurity.org* (7 November 2011) <http://www.globalsecurity.org/military/world/rok/sgr-a1.htm> accessed 17 December 2020.
[211] Robert Sparrow, 'Twenty Seconds to Comply: Autonomous Weapon Systems and the Recognition of Surrender' (2015) 91 International Law Studies 699.
[212] Robert Sparrow, 'Twenty Seconds to Comply: Autonomous Weapon Systems and the Recognition of Surrender' (2015) 91 International Law Studies 718.
[213] *AMW Manual Commentary*, Rule 15(b), 7.

combat".[214] According to Boothby, this means that if an alternative and reasonably available means or method of attack would permit such recognition, the "should be recognized" criterion is satisfied, and if an AWS erroneously proceeds with an attack, the rule is violated.[215] This interpretation of Article 41(1) assumes that the requirement of "feasibility" under Article 57(2)(a)(i) sets the correct standard and, if accepted, would mean that limitations of ATR technologies will not, in themselves, afford an excuse for failing to comply with the principle of distinction. Consequently, commanders will have to consider very carefully their deployment options, even in simple and remote battlefields.

However, there is a compelling counter-argument with Henderson, Keane and Liddy contending that Article 41(1) itself sets the correct standard for determining *hors de combat*.[216] Under their approach, the legal issue is not whether an alternative and reasonably available weapon system would have permitted accurate recognition; but whether, based on the actual weapon system employed, a person should have been recognised as being *hors de combat*. This would appear to be consistent with State practice: means and methods of warfare have long involved indirect fires[217] and, since the 1960s, a range of other 'beyond-visual-range' (BVR) engagements, particularly in air combat.[218] None of these assist attackers in determining whether persons to be engaged are *hors de combat*, yet they continue to be routinely deployed with no legal difficulty. Moreover, as the *AMW Manual Commentary* explains, combatants must effectively communicate their intention to surrender. If they do not, and if attackers conducting a BVR engagement remain unaware of their intention to surrender, the attack may lawfully proceed; so long as the lack of knowledge on the part of the attackers is reasonable in the circumstances.[219]

---

[214] Article 41(1), AP I.
[215] William H. Boothby, 'Autonomous Attack – Opportunity or Spectre?' in Terry D. Gill (ed.), *Yearbook of International Humanitarian Law 2013*, Vol. 16 (TMC Asser Press, 2015), 109.
[216] Ian S. Henderson, Patrick Keane and Josh Liddy, 'Remote and Autonomous Warfare Systems: Precautions in Attack and Individual Accountability' in Jens David Ohlin (ed.), *Research Handbook on Remote Warfare* (Edward Elgar, 2017), 348.
[217] NR. Jenzen-Jones (ed.), *Indirect Fire: A Technical Analysis of the Employment, Accuracy, and Effects of Indirect-Fire Artillery Weapons* (ARES, January 2017), 15-58 <https://www.icrc.org/en/document/indirect-fire-technical-analysis-employment-accuracy-and-effects-indirect-fire-artillery> accessed 17 December 2020
[218] John Stillion, *Trends in Air-to Air Combat: Implications for Future Air Superiority* (CSBA, 2015) <http://csbaonline.org/uploads/documents/Air-to-Air-Report-.pdf> accessed 17 December 2020.
[219] *AMW Manual Commentary*, Rule 15(b), 5.

In view of this, where the sensory limitations of an AWS cause it to fail to detect surrender or incapacitation, this should not in itself render an attack unlawful. To effectively communicate surrender to attacking forces, the burden is on surrendering forces to communicate with the forces conducting an autonomous attack; even if this requires contacting other forces, which can pass the information to the relevant commander in good time.

The issue is even clearer in the ICRC's restatement of customary law, which simply prohibits attacks on "persons who *are* recognized as *hors de combat*", with no alternative "should be recognised" criterion.[220] This is likely to be the default legal position for States not Party to AP I, such as the US and Israel.

Objects

As far as objects are concerned, military objective is defined in Article 52(2), AP I, as:

"[T]hose objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[221]

One of the most heavily debated provisions in AP I,[222] this is often referred to as a two-pronged test in that it comprises two cumulative criteria, as indicated by the conjunctive "and".[223] First, there is the effective contribution to [the enemy's] military action (ECMA) by reference to the nature, location, purpose or use ;[224] second, the "definite military advantage" (DMA) to the attacker, to be assessed "in the circumstances ruling at the time". Both criteria must be fulfilled in light of their qualifiers,[225] though there seems to be no consensus on timing: some argue that both

[220] CIHL, Rule 47.
[221] Article 52(2), AP I; *AMW Manual*, Rule 1(y). See also CIHL, Rule 8.
[222] Stefan Oeter, 'Means and Methods of Combat' in Dieter Fleck (ed.), *The Handbook of International Humanitarian Law* (3rd ed., OUP, 2013), 169. See W. Hays Parks, 'Air War and the Law of War' (1990) 32 Air Force Law Review 1, 135-45; Cf. Judith Gail Gardam, 'Proportionality and Force in International Law' (1993) 87 American Journal of International Law 391, 404-10.
[223] Horace B. Robertson, Jr, 'The Principle of the Military Objective in the Law of Armed Conflict' (1997) 8 United States Air Force Academy Journal of Legal Studies 35, 48.
[224] Gary D. Solis, *The Law of Armed Conflict: International Humanitarian Law in War* (2nd ed., CUP, 2016), 510.
[225] William H. Boothby, *The Law of Targeting* (OUP, 2012), 102.

conditions must be simultaneously present;[226] others seeing no temporal aspect;[227] yet, others taking a middle-ground with a condition of reasonableness.[228]

An accurate understanding of the definition of military objective and its application is indispensable, not only for commanders to know which objects they can legitimately attack, but also for ensuring humanitarian protection. This is because civilian objects, which are immune from direct attack, are defined in the negative.[229] As a general proposition, it is assumed that the broader and/or more concrete the application of each component of the definition, the more amenable it will be to algorithmic determination in the 'narrow loop'.

'Nature' and 'Location'

The *AMW Manual Commentary* explains that an object is a military objective by nature when its "inherent characteristic or attribute" contributes to military action".[230] Examples include military aircraft (including unmanned); military vehicles (excluding medical transports); missile batteries and other weapons; military equipment, fortifications, facilities and depots; warships; and ministries of defence and armaments factories. Crucially for AWS, the military characteristics of these objects are non-changeable, meaning that they "*always* constitute lawful targets during armed conflict…even when not in use".[231] This is further reinforced, both in the *AMW Manual Commentary*[232] and by academic opinion.[233] If accepted, it eliminates the need for context-based evaluation at a given point in time, thus facilitating *ex ante* programming[234] and deployment for both a TS and (tactical-level combat) TLC. The *AP I Commentary* appears to take an even broader view, simply defining military objective by nature as "all objects directly used by the armed

[226] *AP I Commentary*, 2018.
[227] Marco Sassóli, 'Legitimate Targets of Attack Under International Humanitarian Law', *Harvard Program on Humanitarian Policy and Conflict Research, Background Paper* (2003), 7
[228] Ian Henderson, *The Contemporary Law of Targeting: Military Objectives, Proportionality and Precautions in Attack under Additional Protocol I* (Martinus Nijhoff, 2009), 52.
[229] See also *AMW Manual*, Rule 1(j); CIHL Study, Rule 9. The *AP I Commentary*, 2012.
[230] *AMW Manual Commentary*, Rule 22(a), 1.
[231] *AMW Manual Commentary*, Rule 22(a), 1.
[232] *AMW Manual Commentary*, Rule 22(a), 3.
[233] Horace B. Robertson, Jr, 'The Principle of the Military Objective in the Law of Armed Conflict' (1997) 8 United States Air Force Academy Journal of Legal Studies 49.
[234] Yoram Dinstein, 'Legitimate Military Objectives under the Current Jus in Bello' (2002) 78 International Law Studies 139, 146-47.

forces", before providing a relatively short illustrative list;[235] again, facilitating *ex ante* programming. Moreover, given the technical features of ATR, these robust definitions render such objects highly machine-perceptible via a quantitative assessment of inherent, non-changeable and easily-recognisable characteristics, like image, size, shape, sound, heat, velocity and material content. The reliability is further bolstered in the case of cooperative targets, which emit signals that can be easily detected by passive sensors; and by drawing on stationary and/or moving target indication.

Conversely, there is a body of academic opinion, which maintains that a military object is not a military objective by default, and that the former are only targetable if they independently meet the two-pronged test of the latter.[236] In this sense, such opinion diverges from the approach taken in the *AMW Manual Commentary*; not in relation to ECMA *per se*, but in relation to the DMA qualifying the ECMA. Given the two-pronged, cumulative drafting of Article 52(2), it is submitted that this latter view must be correct, with the overall effect that military objects by nature become relatively less amenable at autonomous attack. Conversely, the DMA alone rarely negates the definition of military objective.

An object is a military objective by location when its geographical location makes an ECMA, irrespective of its nature, use, or even purpose.[237] This includes bridges situated in militarily strategic areas, or even a specific area of land *en masse*,[238] where it is important for military operations to seize that location, to deny the enemy from seizing it, or to force the enemy to retreat from it.[239] Accordingly, attacking a location is only lawful under certain circumstances,[240] as every plot of land is unique and may offer a shifting and contextual value for the enemy's military action. This calls for deliberative human input in the determination of which *specific* locations to target.

[235] *AP I Commentary*, 2020.
[236] William H. Boothby, *The Law of Targeting* (OUP, 2012), 103.: Ian Henderson, *The Contemporary Law of Targeting: Military Objectives, Proportionality and Precautions in Attack under Additional Protocol I* (Martinus Nijhoff, 2009), 55.
[237] *AMW Manual Commentary*, Rule 22(b).
[238] Marco Sassóli, Antoine A. Bouvier and Anne Quintin, *How Does the Law Protect in War?: Cases, Documents and Teaching Materials on Contemporary Practice in International Humanitarian Law, Vol. I* (3rd ed., ICRC, 2011).
[239] *AP I Commentary*, 2021.
[240] *AMW Manual Commentary*, Rule 22(b).

Concretely, this means that – unlike military objects by nature that can be engaged in TLC – attacking a location will almost certainly have to be a TS. It will need to benefit from the controlled processing and metacognitive thinking that goes into the deliberate or dynamic targeting cycle, leaving the weapon system to act autonomously only in relation to the timing of the attack and (potentially) the munition selected. It is also likely that, in line with precautionary measures, commanders will have to demarcate the smallest area of land consistent with the requirements of military necessity,[241] and the one whose military utility (for the enemy) is least likely to erode during the time of deployment. However, contrary to the unsupported assertion of the *AP I Commentary*,[242] a location-based military objective is unlikely to be restricted to the immediate combat area,[243] especially when areas outside the contact zone are typically used as logistical routes. There is no obvious reason why this would be any different in the case of an autonomous attack.

Once these legal boundaries are applied and integrated into the targeting process, location becomes the most amenable to machine perception of the four ECMA sub-criteria. Unlike the determination of an object's nature, which calls for stochastic reasoning, a location is objectively ascertainable via the Global Positioning System (GPS). Even in denied areas, where GPS guidance systems may be ineffective or vulnerable to hacking, an AWS will still be able to operate reliably via electro-optical/infrared scene-matching.

To summarise, AWS fitted with appropriate ATR and guidance systems are indeed capable of being deployed in compliance with the nature and location sub-criteria. This is helped by the fact that the effective contribution to military action need not be critical or even significant for an object to qualify as a targetable military objective;[244] so long as it does in fact contribute to the enemy's military action.[245] Arguably, the binary nature of this condition supports the application of

[241] *AP I Commentary*, 2026.
[242] *AP I Commentary*, 2026.
[243] Ian Henderson, *The Contemporary Law of Targeting: Military Objectives, Proportionality and Precautions in Attack under Additional Protocol I* (Martinus Nijhoff, 2009), 56.
[244] Michael N. Schmitt and Eric W. Widmar, 'On Target: Precision and Balance in the Contemporary Law of Targeting', (2014) 7 Journal of National Security Law & Policy 392.
[245] *AMW Manual Commentary*, Rule 1(y), 4.

presumptions over context-based evaluation, thus making it more likely that *ex ante* programming and machine perception will operate in line with legal requirements.

'Purpose' and 'Use': The Problem of 'Dual-Use' Objects

In contrast, the last two ECMA sub-criteria – 'use' and 'purpose' – are more difficult to assess, both for human soldiers and, even more so, for AWS. At their core is the fact that both concepts involve *dual-use objects*; namely, those that simultaneously serve both the military and the civilian population of the enemy. Such an object, "on the face of it, is civilian in nature…but subsequently becomes a lawful target as a result of conversion to military use".[246] Crucially, with simultaneous military and civilian use, an attack can only proceed subject to the principle of proportionality,[247] which presents an extra layer of complexity for an AWS, with perhaps a greater need for controlled processing during the targeting cycle.

While not strictly a legal term, dual-use objects give rise to two distinct factual problems. First, attacks on these objects often have a more perilous effect on civilians, either because the latter are more likely to be present and/or because these attacks tend to inflict damage or pose dangers to them that continue for long periods;[248] though, this is more a policy and legal proportionality concern. Second, and more pertinent to the principle of distinction, both sub-criteria are highly malleable, especially during hostilities; hence, they demand that greater attention be paid to the adjectives effective and definite, to ensure the object being targeted really has acquired the legal status of military objective.

That said, it was noted above that the effective contribution need not be critical or even significant; so long as an ECMA does in fact exist. Furthermore, ECMA does not presuppose a direct connection with combat operations, as is implied in Article 51(3) regarding persons.[249] Thus, Article 52(2) can make a civilian object targetable through 'use' or 'purpose' that is only indirectly related to military action; again, so long as it makes an effective contribution. This relative breadth

[246] *AMW Manual Commentary*, Rule 22(d), 1.
[247] *AP I Commentary*, 2023.
[248] William H. Boothby, *The Law of Targeting* (OUP, 2012), 104.: Judith Gail Gardam, 'Proportionality and Force in International Law' (1993) 87 American Journal of International Law 391, 404.
[249] Michael Bothe, Karl Josef Partsche and Waldemar A. Solf, *New Rules for Victims of Armed Conflict: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949* (Martinus Nijhoff, 1982), 324.

of the ECMA concept can, in some circumstances, make it more amenable to autonomous application, although the bigger picture is that the determination of use and purpose will generally need a greater input of deliberative human reasoning.

'Use' means the enemy is presently utilising the object for military ends,[250] regardless of "its original nature or…any (later) intended purpose",[251] and regardless of the extent of military use.[252] Importantly for an AWS, this latter point makes it a binary concept in that an attacker need only recognise military use but need not measure its degree or intensity. An example of a situation that may be amenable to machine perception is where enemy forces commandeer civilian cars and taxis, to transport troops/supplies, or merely to use these vehicles as cover. If those persons satisfy the three-/four-part criteria for status-based targeting, their perceptible use of civilian vehicles may make the latter a military objective by 'use', regardless of the extent of that use. However, where a civilian is driving a truck which, in the circumstances is a military objective, the truck (not the driver) can be targeted even if it results in the death of the driver. Similar reasoning may apply to some other civilian objects like dwellings, a hotel or a school (for troop accommodation, for taking cover, or as observation points)[253], or bridges (for vehicle and troop movements). Insofar as these objects are utilised transparently by enemy combatants, they may become targetable by an AWS during TLC.

However, in other cases military use can be relatively opaque. For example, power grids and computer hardware and software are unpredictably malleable during an armed conflict, and it is often unclear who is using them.[254] The same can be said of dwellings and other civilian buildings, when used in discreet ways (as a military storage facility via underground tunnels). In yet other cases, the problem is less opacity and more a lack of machine-perceptibleness: consider a civilian broadcast facility used for military transmission and enemy propaganda.[255] AWS algorithms will

[250] *AP I Commentary*, 2022.
[251] Yoram Dinstein, 'Legitimate Military Objectives under the Current Jus in Bello' (2002) 78 International Law Studies 149.
[252] Michael N. Schmitt and Eric W. Widmar, 'On Target: Precision and Balance in the Contemporary Law of Targeting', (2014) 7 Journal of National Security Law & Policy 393.
[253] *AP I Commentary*, 2022; *AMW Manual Commentary*, Rule 22(d), 2.
[254] Marco Sassóli, 'Legitimate Targets of Attack Under International Humanitarian Law', *Harvard Program on Humanitarian Policy and Conflict Research, Background Paper* (2003), 7.
[255] Office of the Prosecutor, *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia* (2000) 39 ILM 1257, 71.

be trained in advance and in relatively abstract settings, yet it is difficult – if not impossible, in the case of computers – to identify when, how and in which context these objects are destined for military use.[256] Similar difficulty will bedevil an AWS in assessing when discreet (or machine-imperceptible) military use comes to an end, at which point the object ceases to be a lawful target and may no longer be attacked.[257] Accordingly, the pliable concept of use at any given moment – already very challenging for human combatants to apply – will be nigh-on impossible for an AWS to assess in the midst of TLC, and in situations of opacity and imperceptibleness.

'Purpose' takes this difficulty to the next level, as it refers to the intended future use of an object.[258] Accordingly, 'purpose' is determined after the crystallisation of the original 'nature' of an object, but before its actual 'use'.[259] This permits the targeting of a civilian object in between uses, and even prior to initial use,[260] thus recognising that an attacker need not wait for a civilian object to actually be utilised for military ends before striking it.[261] Tempering this, however, is a requirement that there be a 'reasonable belief' of actual intended future use, not just the mere potential or objective possibility for it.[262] As Dinstein asserts:

"Purpose is predicated on intentions known to guide the adversary, and not on those figured out hypothetically in contingency plans based on a 'worst case scenario'."[263]

At the very least, determining the enemy's future intention requires knowledge of its Tactics, Techniques and Procedures, and the gathering and analysis of intelligence.[264] Even then, reaching a firm and reliable conclusion is not always easy. Sometimes, enemy intentions are "crisply clear",

[256] Marco Sassóli, 'Legitimate Targets of Attack Under International Humanitarian Law', *Harvard Program on Humanitarian Policy and Conflict Research, Background Paper* (2003), 7.
[257] *Manual Commentary*, Rule 22(d), 4.
[258] *AP I Commentary*, 2022.: See also *AMW Manual Commentary*, Rule 22(c), 1.
[259] Yoram Dinstein, 'Legitimate Military Objectives under the Current Jus in Bello' (2002) 78 International Law Studies 148.
[260] Ian Henderson, *The Contemporary Law of Targeting: Military Objectives, Proportionality and Precautions in Attack under Additional Protocol I* (Martinus Nijhoff, 2009), 59.
[261] *AMW Manual Commentary*, Rule 22(c), 1.
[262] William H. Boothby, *The Law of Targeting* (OUP, 2012), 103.
[263] Yoram Dinstein, 'Legitimate Military Objectives under the Current Jus in Bello' (2002) 78 International Law Studies 148.
[264] Lieutenant Colonel Christopher M. Ford, 'Autonomous Weapons and International Law' (2017) 69 South Carolina Law Review 440.

as in the case of overtly-announced plans; other times, intentions are "not so easy to decipher", and will require relatively more painstaking intelligence efforts in advance.[265] This latter scenario entails the assembly of fragmented pieces of information, often of varying degrees of reliability and with no coherent picture.[266] Hence, there is a need to assess a) the reliability of intelligence; and b) either what is missing and where to obtain it, or "conjecture to fill in the missing pieces of the puzzle". To add further to the cognitive task, conjecture itself must remain consistent with the 'reasonable belief' standard.[267]

This all leads to two pertinent conclusions. First, the determination of a military objective by purpose clearly calls for autonoetically metacognitive thinking, which is a uniquely human domain. This is underscored by the *AMW Manual Commentary*, which advises that:

"The attacker must always act reasonably…[and] ask itself whether it would be reasonable to conclude that the intelligence [regarding future intentions] was reliable enough to conduct the attack in light of the circumstances ruling at the time."[268]

Applying such broad standards as 'reasonableness' to concrete facts, along with the degree of introspection implied here, involves higher-order thinking skills that will arguably not be automated in the near-term.

The second conclusion is that the above account of intelligence activities to establish 'purpose' would seem to describe the kinds of tasks that occur in the deliberate targeting process; in particular, during Phase 2 (target development). Accordingly, the difficulty of establishing enemy intentions and the 'purpose' of an object does not necessarily preclude an AWS from engaging such objects. Indeed, human pilots currently do not attempt to establish the 'purpose' of an object, but instead operate their planes and weapon systems to complete missions in accordance with the

[265] Yoram Dinstein, *The Conduct of Hostilities Under the Law of International Armed Conflict* (3rd ed., CUP, 2016), 114.
[266] *AMW Manual Commentary*, Rule 22(c), 3.
[267] William H. Boothby, *The Law of Targeting* (OUP, 2012), 104.
[268] *AMW Manual Commentary*, Rule 22(c), 3.

'target package' provided to them.[269] The higher-order thinking therefore takes place during the earlier phases of the largely human-controlled targeting cycle, with the human pilot merely executing a TS. Even in a dynamic targeting scenario, pilots are briefed with necessary information to engage a target that has, nonetheless, been subjected to considerable human analysis and pre-selected by other specialist personnel. Arguably, there is no reason to believe that an AWS cannot engage a military objective by purpose in the same way.

'Use' and 'purpose' both make clear that LOAC incorporates a dynamic element, as civilian objects are liable to become military targets depending on the plans, actions and behaviours of both parties.[270] Unlike the analysis of large military objectives by nature or location, both of which rely more on quantitative matching (automatic processing), the legitimacy of attacking much of the above is highly fluid and context-dependent. This points to sophisticated qualitative analysis (controlled processing) to which humans are predisposed,[271] and this situation is likely to remain true for the foreseeable future.

However, contrary to assertions that this makes AWS unlawful, risky or of limited military value, it merely requires that military objectives by use and purpose be engaged in a TS; or, at most, that AWS ROE be restricted to military objectives by nature and location. Arguably, these restrictions are not too onerous because, in practice, most attacks are based on an object's nature (in TLC) or use (in a TS),[272] thereby accommodating AWS deployments.

The 'Definite Military Advantage in the Circumstances Ruling at the Time'

Once the first (ECMA) criterion is satisfied, another difficulty may still present itself in the second criterion to be assessed: that the destruction of an object must offer (to the attacker) a 'definite military advantage' (DMA) in 'the circumstances ruling at the time'.[273]

---

[269] Merel Ekelhof, 'Autonomous Weapons: Operationalizing Meaningful Human Control', *ICRC Humanitarian LAW & Policy* (15 August 2018) <http://blogs.icrc.org/law-and-policy/2018/08/15/autonomous-weapons-operationalizing-meaningful-human-control/> accessed 21 December 2020.
[270] Markus Wagner, 'Autonomy in the Battlespace: Independently Operating Weapon Systems and the Law of Armed Conflict' in Dan Saxon (ed.), *International Humanitarian Law and the Changing Technology of War* (Martinus Nijhoff, 2013), 112.
[271] Markus Wagner, 'The Dehumanization of International Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapon Systems' (2014) 47 Vanderbilt Journal of Transnational Law 1393.
[272] *AMW Manual Commentary*, Rule 22, 2.
[273] Article 52(2), AP I; *AMW Manual*, Rule 1(y); CIHL, Rule 8.

This second prong requires that the military advantage to the attacking party be definite, not merely "potential or indeterminate";[274] lest an excessive range of objects become open to attack.[275] Yet, the DMA need not directly flow from the attack;[276] nor must it offer immediate tactical gain, but it can be an "operational advantage accruing to the larger campaign".[277]

On the one hand, some commentators consider that this merely duplicates the first criterion,[278] such that the two "mostly presuppose each other".[279] If not always, then at least "most objects" will fulfil both prongs "[a]s a practical matter".[280] If so, an AWS that is able to meet the first criterion will likely satisfy the principle of distinction *vis-à-vis* objects.

On the other hand, the *AP I Commentary*[281] and several academic commentators[282] take a different view, focusing on the temporal aspect of the second criterion.[283] If this interpretation is accepted, it may require that tactical AWS units be fed constant updates from the commander on the circumstances of the military operation and its evolution:[284] a requirement that at first blush might seem too onerous, perhaps even undermining the purpose of weapons autonomy. That said, such temporal distinctions are generally rare and occur more as an aberration. In addition, it is arguable that all military objectives by nature can be assumed, by default, to also be military objectives by

[274] *AP I Commentary*, 2024.
[275] Ian Henderson, *The Contemporary Law of Targeting: Military Objectives, Proportionality and Precautions in Attack under Additional Protocol I* (Martinus Nijhoff, 2009), 63.
[276] Michael Bothe, Karl Josef Partsche and Waldemar A. Solf, *New Rules for Victims of Armed Conflict: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949* (Martinus Nijhoff, 1982), 324.
[277] Michael N. Schmitt and Eric W. Widmar, 'On Target: Precision and Balance in the Contemporary Law of Targeting', (2014) 7 *Journal of National Security Law & Policy* 392.
[278] Yoram Dinstein, *The Conduct of Hostilities Under the Law of International Armed Conflict* (3rd ed., CUP, 2016), 104.
[279] Janina Dill, *Legitimate Targets? Social Construction, International Law and US Bombing* (CUP, 2015), 71.
[280]See also *AMW Manual Commentary*, Rule 1(y), 3.
[281] *AP I Commentary*, 2018.:
[282] Remarks by Françoise J. Hampson, 'Proportionality and Necessity in the Gulf Conflict' (1992) 86 Proceedings of the Annual Meeting (American Society of International Law) 49.: Timothy LH. McCormack and Helen Durham, 'Aerial Bombardment of Civilians: The Current International Legal Framework' in Yuki Tanaka and Marilyn B. Young (eds.), *Bombing Civilians: A Twentieth-Century History* (The New Press, 2009), 222-24.
[283] Timothy LH. McCormack and Helen Durham, 'Aerial Bombardment of Civilians: The Current International Legal Framework' in Yuki Tanaka and Marilyn B. Young (eds.), *Bombing Civilians: A Twentieth-Century History* (The New Press, 2009), 223.
[284] Nathalie Weizmann, 'Autonomous Weapon Systems under International Law', *Academy Briefing No. 8* (Geneva Academy of International Humanitarian Law and Human Rights, November 2014), 14.

purpose, so long as they are not completely battle-damaged. This is because of the risk that abandoned military objects may be reoccupied by the enemy and put back to military use,[285] or (if partially damaged) utilised for spare parts. Thus, the second (temporal) criterion may be less relevant to such objects, enabling an AWS to engage them without needing to undertake complex value judgments.

Civilian Objects and Specifically Protected Objects

Once the criteria for military objectives are delineated and applied in an AWS context, civilian protection becomes easier. Like the analogous provision for persons, Article 52(1), AP I, prohibits making civilian objects "the object of attack or of reprisals".[286] Again, the nature and wording of this prohibition renders compliance relatively simple: a matter of *ex ante* programming and appropriate deployment,[287] which should pose no difficulty for commanders acting in good faith. The main problem is when a civilian object is being used for a military purpose. Subsequent AP I rules protect specific objects the destruction of which would have an indirectly detrimental effect on civilians. In relation to these, some authors have commented on the limits to machine perception and have queried how AWS will respect these rules.[288] Yet, on closer examination, these prohibitions can also (largely) be seen as programming and deployment matters, which may be expected to pose little or no difficulty for commanders utilising the Joint Targeting process and acting in good faith.

Cultural Property

For example, Article 53(a), AP I, prohibits "acts of hostility directed against…historic monuments, works of art or places of worship".[289] The adverb 'directed' clearly goes to deliberate human

[285] See Joint Readiness Training Center, 'Operation OUTREACH: Tactics, Techniques, and Procedures', *News Letter No. 03-27* (October 2003).
[286] Article 52(1), AP I.
[287] Michael N. Schmitt, 'Autonomous Weapons Systems and International Law', *LENS Conference 2016: Autonomous Weapons in the Age of Hybrid War* (27 February 2016) <https://www.youtube.com/watch?v=b5mz7Y2FmU4> accessed 11 December 2020.
[288] Ozlem Ulgen, 'Definition and Regulation of LAWS' *Submission to April 2018 GGE* (5 April 2018), 11 <https://www.researchgate.net/publication/324227191_Dr_Ulgen_UN_GGE_LAWS_April_2018_-_submission_-_Definition_and_Regulation_of_LAWS> accessed 21 December 2020.
[289] Article 53(a), AP I; *AMW Manual Commentary*, Rule 95(a).

choices made during the targeting cycle, and the same can be said about Paragraph (c), which prohibits "mak[ing] such objects the object of reprisals".[290]

However, the ICRC's restatement of customary law goes further than AP I, and states that: "Special care must be taken in military operations to avoid damage to buildings dedicated to religion, art, science, education or charitable purposes and historic monuments unless they are military objectives."[291]

In an AWS context, much of this 'special care' will begin at Phase 2 of the deliberate targeting cycle. For example, using the UNESCO World Heritage List[292] and World Heritage in Danger List,[293] targeteers have an immediate and authoritative basis to enter high-priority sites on the no-strike list, which an AWS would respect by avoiding any attacks on the relevant GPS coordinates (immovable cultural property) and/or image matches (movable or immovable). Of course, not all cultural sites benefit from a UNESCO listing, so attacking forces may also have to consult other lists. In many cases, however, the most comprehensive and relevant lists of protected heritage (and other protected buildings and monuments) are in the hands of the host State, which has no specific obligation to provide that information to its adversary.[294] On the other hand, there may be a general obligation to do this under Article 58, AP I, if not under the Article 1(1), AP I, obligation to respect and to ensure respect for LOAC *erga omnes*.

Perhaps a better option, which is relatively within the control of attacking forces, is to work with archaeologists to identify all relevant sites that merit protection[295] and to begin this process even before commencement of the formal targeting process, if willing experts can be found.[296] Separately, where a protected object is characterised by distinctive architecture, this may be amenable to the object recognition of an ATR, thus avoidable even in the absence of any list.

---

[290] Article 53(c), AP I.
[291] CIHL, Rule 38(A).
[292] 'World Heritage List' <https://whc.unesco.org/en/list/> accessed 21 December 2020.
[293] 'List of World Heritage in Danger' <https://whc.unesco.org/en/danger/> accessed 21 December 2020.
[294] Marina Lostal, Kristin Hausler and Pascal Bongard, 'Armed Non-State Actors and Cultural Heritage in Armed Conflict' (2017) 24 International Journal of Cultural Property 407, 419-20.
[295] Peter Stone, 'The Identification and Protection of Cultural Heritage During the Iraq Conflict: A Peculiarly English Tale' (2005) 79.
[296] John Curtis, 'Relations Between Archaeologists and the Military in the Case of Iraq' in Peter G. Stone (ed.), *Cultural Heritage, Ethics and the Military* (Boydell Press, 2011).

Where cultural property becomes a military objective,[297] the *AMW Manual Commentary* advises that the decision to attack be taken by an "appropriate level of command", which is taken to mean at least an air squadron or battalion commander.[298] Further, such a decision is to be made with due consideration of its special character as cultural property, as such decisions cannot be taken lightly. This clearly involves complex value judgments, which implicate human metacognitive thinking and discretion; again going back to the human-led targeting process in deploying AWS for a TS. Namely, attacks on cultural property cannot be lawfully executed through generalised parameters programmed for TLC, as the automatic processing of the control software will not be able to make the necessary value judgments.

Objects Indispensable for Civilian Survival

Article 54(2) prohibits attacks against "objects indispensable to the survival of the civilian population…for the specific purpose of denying them for their sustenance value".[299] Once again, the wording of the provision clearly indicates human choices made through the targeting cycle. This is underscored by the UK's and France's statements of interpretation upon ratifying AP I that Article 54(2) does not apply to attacks carried out for a specific purpose other than denying sustenance to the civilian population.[300] Moreover, the *AMW Manual Commentary* emphasises the need for a specific purpose and precludes "incidental distress of civilians resulting from otherwise lawful military operations".[301] Accordingly, so long as commanders – supported by multiple battle staffs and legal advisers, and overseen by the Joint Targeting Coordination Board – do not deploy AWS to attack such indispensable objects for the specific purpose of denying sustenance to the civilian population, or as a reprisal, compliance with Article 54(2) should be relatively easy.

Infrastructure That May Release Dangerous Forces

Article 56(1) prohibits making the object of attack "[w]orks or installations…[that] may cause the release of dangerous forces and consequent severe losses among the civilian population", even if

[297] CIHL, Rule 38(B); and *AMW Manual Commentary*, Rule 95(b).
[298] *AMW Manual Commentary*, Rule 96, 5.
[299] Article 54(2), AP I; *AMW Manual*, Rule 97(b).
[300] UK, Reservations and Declarations Made Upon Ratification of AP I (28 January 1998), Statement (l); France, Reservations and Declarations Made Upon Ratification of AP I (11 April 2001), ¶ 14.
[301] *AMW Manual Commentary*, Rule 97(b), ¶ 2.

such works or installations are military objectives.[302] As with the last two prohibitions, this one also does not pose insurmountable compliance difficulty for an AWS-deploying Belligerent, which utilises a formal targeting process. First, it is significant that the protection from direct attack is limited to three specific types of infrastructure: dams, dykes and nuclear electrical generating stations.[303] Together with the cumulative nature of the criteria[304] and the focus on *ex ante* scrutiny,[305] this limits the burden on intelligence analysts during Phase 2 of the deliberate targeting cycle (or the target stage of the dynamic cycle), and it should facilitate the compilation of a definitive list of such objects and their precise locations. Second, the protection is unique in that it continues even when the works or installations are put to military use and thus glaringly constitute military objectives.[306] Arguably, the combined effect of these two factors is to create an administrable no-strike category: a set of a binary actions that are amenable to both pre-deployment programming and in-field machine perception via GPS guidance systems.[307]

Furthermore, given the possibility to integrate collateral damage estimation capabilities into AWS, this argument may even extend to the second prohibition in Article 56(1), against attacking other nearby military objectives, if such an attack may also cause the release of dangerous forces and consequent severe civilian losses. Thus, underlying the prohibition is a worst case analysis, which assumes that such attacks will induce massive risks to the civilian population. Specifically, these risks are assumed to be a) unacceptably high, b) almost never outweighed by military advantage and, thus, c) cannot be justified by any claim of military necessity, except under the three specific exceptions in Article 56(2).[308] Again, the specificity of the rule may be expected to support machine application.

The fact that protection under Article 56(1) is qualified by the verb 'may' and the adjective 'severe' does not imply that an AWS will have to undertake any value judgments. Rather, as the *AP I*

[302] Article 56(1), AP I. See also *AMW Manual*, Rule 36; CIHL, Rule 42.
[303] *AP I Commentary*, 2147-2150.
[304] Leslie C. Green, *The Contemporary Law of Armed Conflict* (2nd ed., MUP, 2000), 158 .
[305] Frits Kalshoven, *Reflections on the Law of War: Collected Essays* (Martinus Nijhoff, 2007), 235.
[306] Yoram Dinstein, *The Conduct of Hostilities Under the Law of International Armed Conflict* (3rd ed., CUP, 2016), 227.
[307] William H. Boothby, 'Autonomous Attack – Opportunity or Spectre?' in Terry D. Gill (ed.), *Yearbook of International Humanitarian Law 2013*, Vol. 16 (TMC Asser Press, 2015), 81.
[308] Stefan Oeter, 'Means and Methods of Combat' in Dieter Fleck (ed.), *The Handbook of International Humanitarian Law* (3rd ed., OUP, 2013), 218.

Commentary points out, 'severe' (losses among the civilian population) is a matter of 'common sense' and is to be applied in 'good faith' on the basis of objective criteria, such as population density and the proximity of inhabited areas. Accordingly, commanders and their battle staffs are to make these judgment calls when deciding which specific objects and locations to put on the no-strike list, which an AWS will simply be programmed not to attack.

Arguably, the same is true with respect to the specific grounds on which protection from attack shall cease under Article 56(2). These require that a) the work, installation or nearby military objective is used in regular, significant and direct support of military operations, and b) that an attack is the only feasible way to terminate such support. This sets the bar significantly higher than the effective contribution to military action that an object must make to qualify as a military objective under Article 52(2) and it calls for a commander at the highest military level to make the judgment call, usually based on prior intelligence. This again points to the deliberate (or at least the dynamic) targeting cycle in reaching a deliberative human decision to conduct an attack pursuant to Article 56(2), while a narrow loop AWS will merely execute the attack via TS, and will *refrain* from such actions at all other times.

Medical Capabilities

The protection of medical capabilities to treat the sick, wounded and shipwrecked is a particular concern in IHL/LOAC, and is an essential component of efforts to humanise war. To this end, there are specific distinction-based AP I rules that afford respect for, and protection to:

- Fixed and mobile medical units,[309] with Parties to the conflict being encouraged to notify each other of the locations of fixed units.[310]
- Medical vehicles used exclusively for transportation.[311]
- Hospital ships and coastal rescue craft.[312]
- 'Other' medical ships and craft.[313]

[309] Article 12(1), AP I; Article 19, GC I; Article 18, GC IV; CIHL, Rule 28.
[310] Article 12(3), AP I; *AMW Manual*, Rule 73.
[311] Article 21, AP I; Article 35, GC I; Article 38, GC II; Article 21, GC IV; CIHL, Rule 29.
[312] Article 22, AP I; Articles 22, 24, 25, 27 and 28, GC II; CIHL, Rule 28.
[313] Article 23, AP I, also expanding on analogous provisions in GC II.

- Medical aircraft.[314]

Like the previous prohibitions, these are also simple programming and deployment matters. However, as the *AMW Manual Commentary* points out, to respect medical personnel and facilities is broader than simply refraining from directly attacking them, and it includes a prohibition against "unnecessarily preventing them from discharging their functions".[315] Thus, an AWS would have to be programmed to, for example, keep a distance from such facilities, lest it inadvertently creates a fear of impending attack, thereby disrupting medical operations. Crucially, recognition of protected status – an essential prerequisite for respecting it – can be greatly enhanced via technical means, which exploit the strengths of automatic processing.

Enhancing Detection by Technical Means

First, as noted above, whenever the location of a fixed protected object is known, respect will be effectuated primarily by assigning a no-strike categorisation to its GPS coordinates.[316] Beyond this, and in the case of unknown or movable objects, there are additional safeguards, which may support autonomous attack and make it more discriminating. These include:

- The Blue Shield that denotes cultural property.[317]
- The international special sign (three bright orange circles) for works and installations containing dangerous forces.[318]
- The distinctive emblems of the Red Cross and Red Crescent,[319] which denote medical and religious personnel and facilities.[320]

Importantly, these can all be specifically designed to facilitate detection by the ATR of an AWS; for example, using ancillary lighting, thermal ribbons and detailed colour contrasts.[321]

---

[314] Article 24, AP I; Article 36, GC I; Article 39, GC II; CIHL, Rule 28. *AMW Manual*, Rule 72(a).
[315] *AMW Manual Commentary*, Rule 71, 12.
[316] William H. Boothby, 'Autonomous Attack – Opportunity or Spectre?' in Terry D. Gill (ed.), *Yearbook of International Humanitarian Law 2013*, Vol. 16 (TMC Asser Press, 2015), 81.
[317] Articles 6, 10, 16, 17 and 20, Convention for the Protection of Cultural Property in the Event of Armed Conflict (adopted 14 May 1954, entered into force 7 August 1954) 249 UNTS 240.
[318] Article 56(7), AP I; Article 17, Amended Annex I.
[319] Article 4, Amended Annex I; CIHL, Rule 30.
[320] Article 18, AP I
[321] Article 17(4), Amended Annex I.; See also *AMW Manual Commentary*, Rule 72(b).

Furthermore, there is a range of 'distinctive signals' for the exclusive use of medical units and transports; for example, the distinctive light signal, radio signals and radio messages, and various forms of electronic identification. Each is individually predisposed to relatively reliable detection by technical means, and in combination with each other and with the distinctive emblems, they offer an invaluable means of detection-confirmation. These will further enhance the distinction capabilities of an AWS, and help to avoid the kinds of unintended engagements seen with manned targeting.[322]

That said, attacking forces must remain vigilant and avoid any over-reliance on emblems, signs and signals. Indeed, placing too much faith in these safeguards – and in human efforts to deploy them fully and accurately – may lead to a watering down of commander-led targeting efforts and, ultimately an increase in distinction failure.

Enhancing Confidence in Technical Detection

Helping to enhance the confidence of attacking forces in their ATR assessments, Article 38, AP I, prohibits adverse Parties from making any improper use of emblems, signs or signals;[323] for example, by attaching them to military objectives. Moreover, should such improper use become perfidious, this will elevate the violation to a gross breach of AP I and, therefore, a war crime.[324] The discussion on perfidy in previous section applies equally here, including the likelihood that adversarial examples, which merely imitate the recognised emblems, signs or signals, will be sufficient to establish a violation.

Will AWS be Able to Sense Targeting 'Doubt'?

The decision to attack is often based on incomplete or inconclusive information. The resulting uncertainty (or 'fog of war'), which pervades armed conflict raises the question: "how certain must

[322] See 'ICRC Warehouses Bombed in Kabul', *ICRC News Release 01/43* (16 October 2001) <https://www.icrc.org/eng/resources/documents/news-release/2009-and-earlier/57jrcz.htm>; 'Bombing and Occupation of ICRC Facilities in Afghanistan', *ICRC News Release 01/48* (26 October 2001) <https://www.icrc.org/eng/resources/documents/news-release/2009-and-earlier/57jrdx.htm>; 'Kunduz Bombing: US Attacked MSF Clinic 'In Error'', *BBC News* (25 November 2015) <http://www.bbc.co.uk/news/world-asia-34925237>; all accessed 21 December 2020.
[323] Article 38, AP I; *AMW Manual*, Rule 112(a)-(b); CIHL, Rules 59-61.
[324] Article 85(3)(f), AP I.

[an attacker] be that the object or person is a lawful target before proceeding?"[325] As a matter of law, both the question and its answer are crucial, as AP I mandates that in the event of 'doubt', civilian status shall be presumed for persons.[326]In the case of objects, the object has to be normally civilian for the presumption to apply,[327] thereby protecting them from direct attack. Importantly, this presumption relates to civilian status and is not a conduct-based presumption against DPH. In relation to objects, the language of the AP I norm is reproduced in Amended Protocol II,[328] which regulates the use of anti-personnel mines. Significantly, these weapons also operate with humans out-of-the-narrow-loop, thereby underscoring the need to act on doubt in such circumstances. With these in mind, the *AMW Manual Commentary* fully extends the rule of doubt to autonomous lethal targeting,[329] where it will be a prominent factor in both the development and deployment of AWS.[330]

That said, the degree of doubt required to trigger the presumption of civilian status is not codified in treaty law, and with varying State practice there is arguably no customary standard.[331] To be sure, war is replete with uncertainty, and the mere existence of some doubt is insufficient to preclude an attack;[332] rather, as the *AP I Commentary* makes clear, 'doubt' is likely to be context-specific.[333] Accordingly, the ICTY Trial Chamber in *Galić* articulated the legal standard as:

---

[325] Ian Henderson and Bryan Cavanagh, 'Unmanned Aerial Vehicles (UAVs): Do They Pose Legal Challenges?' in Hitoshi Nasu and Robert McLaughlin (eds.), *New Technologies and the Law of Armed Conflict* (TMC Asser Press, 2014), 204.
[326] Article 50(1), AP I: "In case of doubt whether a person is a civilian, that person shall be considered to be a civilian." See also CIHL, Rule 6.
[327] Article 52(3), AP I: "In case of doubt whether an object which is normally dedicated to civilian purposes…is being used to make an effective contribution to military action, it shall be presumed not to be so used." See also CIHL, Rule 10.
[328] Article 3(8)(a), Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices (adopted 10 October 1980, amended 3 May 1996, entered into force 3 December 1998) 2048 UNTS 93.
[329] *AMW Manual Commentary*, Rule 39, 5 ("The standards…regarding doubt apply equally to UCAV attacks, *whether autonomous or manned*")
[330] Jeffrey S. Thurnher, 'Means and Methods of the Future: Autonomous Systems' in Paul AL. Ducheine, Michael N. Schmitt and Frans PB. Osinga (eds.), *Targeting: The Challenges of Modern Warfare* (TMC Asser Press, 2016), 191.
[331] Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed., CUP, 2017) (hereafter, *Tallinn Manual 2.0*), Rule 95, 3.
[332] *Tallinn Manual 2.0*, Rule 95, ¶ 3 (persons) and Rule 102, ¶ 9 (objects); *AMW Manual Commentary*, Rule 12(a), ¶ 4 (persons) and Rule 12(b), ¶¶ 4 and 5 (objects).
[333] *AP I Commentary*, ¶ 1920

'…when it is not reasonable to believe, in the circumstances of the person contemplating the attack, including the information available to the latter, that the potential target is a combatant [or an object being used to make an effective contribution to military action].'[334]

The *AMW Manual Commentary* echoes this,[335] as does the 'positive identification' (PID) standard set out in some ROE, which requires 'a reasonable certainty that the proposed target is a legitimate military target'. [336] Henderson and Cavanagh therefore argue that 'reasonable belief' and 'reasonable certainty' are practically synonymous and, when considered in the circumstances of the attacker – including the information or intelligence available to him – provide a sufficiently clear and practical test; at least for a metacognitive human.[337]

In an AWS context, this means where there is enough doubt that a reasonable human attacker – possessing the same information and in *a* similar situation as the *AWS* – would hesitate, then an attack will not legally be allowed to proceed.[338] In such a case of uncertainty, the AWS must be programmed to a) recognise the situation of 'doubt' that would cause a human to hesitate and b) abort the attack,[339] or at least contact a human operator for further instructions.

This framing of doubt in human reasonableness terms will complicate translation into an AWS context. A significant challenge will be to develop an automated mechanism that a) accurately gauges doubt, and b) reliably factors in the unique situation in which the AWS is operating.[340] In this regard, the Trial Chamber in *Galić* noted that observations relating to the clothing, activity,

---

[334] *Prosecutor* v. *Galić* (ICTY Trial Judgment) IT-98-29-T (5 December 2003), ¶ 50 (persons), ¶ 51 (objects), (emphasis added). See also ¶ 55

[335] *AMW Manual Commentary*, Rule 12(a), 4.

[336] See CFLCC and MNC-I ROE Cards, reprinted in LCDR David H. Lee (ed.), *Operational Law Handbook* (JAG's Legal Center & School, US Army, 2015), 109-10

[337] Ian Henderson and Bryan Cavanagh, 'Unmanned Aerial Vehicles (UAVs): Do They Pose Legal Challenges?' in Hitoshi Nasu and Robert McLaughlin (eds.), *New Technologies and the Law of Armed Conflict* (TMC Asser Press, 2014), 205.

[338] Jeffrey S. Thurnher, 'Means and Methods of the Future: Autonomous Systems' in Paul AL. Ducheine, Michael N. Schmitt and Frans PB. Osinga (eds.), *Targeting: The Challenges of Modern Warfare* (TMC Asser Press, 2016), 192.

[339] Nathalie Weizmann, 'Autonomous Weapon Systems under International Law', *Academy Briefing No. 8* (Geneva Academy of International Humanitarian Law and Human Rights, November 2014), 14.

[340] Michael N. Schmitt, 'Autonomous Weapons Systems and International Law', *LENS Conference 2016: Autonomous Weapons in the Age of Hybrid War* (27 February 2016) <https://www.youtube.com/watch?v=b5mz7Y2FmU4> accessed 11 December 2020.

age, or gender are relevant when determining whether a person is a civilian[341] and, therefore, whether there is enough doubt to trigger the presumption of civilian status. However, it is not clear how amenable to automatic processing these will be in any given battlefield. Certainly, in the most dynamic battlefields there will potentially be relevant factors that are not foreseen by programmers (or by case law), but to which metacognitive human combatants would be able to improvise.

It should be noted that in relation to objects, the rule is not about doubt in general, but specifically about whether a civilian object is being put to military use. In that regard, the *Tallinn Manual 2.0* points out that in establishing doubt versus the reasonableness of an assessment of military use, an attacker should consider:

"[T]he apparent reliability of the information, including the credibility of the source or sensor, the timeliness of the information, the likelihood of deception, and the possibility of misinterpretation of data."[342]

Namely, in case of any doubt as to whether a civilian object is making an ECMA by use, it may only be attacked after a careful assessment of the situation.[343] This clearly calls for the marshalling of higher-order metacognitive skills, which an AWS will not possess. It was one of the reasons argued previously, for why military objectives by use (or purpose) are likely to be engaged only via a TS. Namely, the need for extensive intelligence analysis and human deliberation will likely demand the rigours of the deliberate (or at least the dynamic) targeting cycle, led by human decision-makers.

On the other hand, more machine-perceptible instances of military 'use' are detected, this may be amenable to autonomous attack. Specifically, in relation to aircraft, the *AMW Manual Commentary* provides an illustrative list of factors, which are potentially relevant to recognising 'doubt' in air warfare.[344] In a similar vein, Arkin discusses recognition of uncertainty through a weighted average of discrete values, e.g. binary (absent or present), or categorical (absent, weak, medium,

[341] *Prosecutor* v. *Galić* (Trial), 50.
[342] *Tallinn Manual 2.0*, Rule 102, 8.
[343] See also CIHL, Rule 10
[344] *AMW Manual Commentary*, Rule 40, 4 (a)-(i)

strong); or real continuous values.[345] This may also combine with 'conservative use of lethal force', where an AWS – not affected by any survival instinct – can hold fire to resolve doubt.

Ultimately, whether an AWS can administer targeting doubt to the legally required standard will – like much of the above analysis – depend on the system, the task being programmed and the operational environment. The more complex and dynamic the task and environment, the more likely the system will be legally non-compliant for lack of controlled processing. Conversely, the simpler and more static the task and environment, the more likely targeting doubt can be resolved through overlapping criteria and statistical confidence thresholds (i.e. automatic processing). Perhaps the more important 'doubt' that needs to be taken into account is that of the commander, when deploying systems into specific missions.

Summary

Distinction is undoubtedly one of the most important of IHL norms, yet it is clearly not easy to comply with in every situation. Yet, by using common sense and acting in good faith, commanders can in principle find suitable restrictions and precautions as to deploy AWS appropriately, and in a way that adequately distinguishes lawful from unlawful targets. Of course, this assumes a) effective training of commanders, and full knowledge on both the capabilities and limitations of prevailing ATR systems, and b) a degree of self-restraint on the part of those commanders, who may be operating under extraordinary operational pressures. Arguably, neither of these conditions will necessarily hold true all of the time, and certainly not on all sides of an armed conflict. Thus, while compliance with the principle of distinction is possible, this will only result from assiduous and well-informed advance decision-making by genuinely accountable commanders.

Guaranteeing AWS Compliance with LOAC: Using Dynamic Diligence

To appropriately handle the practical and doctrinal challenges of AWS accountability, LOAC requires the application of dynamic diligence. Dynamic diligence means that the rules which govern the AWS' operating procedures must have some flexibility, leaning towards being able to interpret its results and make alterations as necessary. To apply dynamic diligence, commanders

[345] Ronald C. Arkin, *Governing Lethal Behaviour in Autonomous Robotics* (Chapman & Hall/CRC, 2009), 59.

must be informed about, and engaged in, the operational performance of an AWS in its past, present and future missions. During the weapons review phase, an AWS should only be approved on the basis of significant and enduring human involvement in its operation. This involvement is, however, limited. The use of dynamic diligence would not necessitate *ex ante* approval of an AWS' target selection. This approach would, however, require ongoing and regular assessment of the its operation, along with adjustments of its programming, outputs and human operator interaction, where appropriate.[346]

Such human involvement satisfies the general understanding of the term 'meaningful human control.'[347] In terms of its general understanding, meaningful human control would not permit the use of 'set and forget' software in any AWS capable of delivering deliberate lethal force. This approach is not sufficiently cautious of the key benefit of AWS: their self-learning ability. Further, it does not consider the risk of this functionality developing into a curse that could cause LOAC violations.

Albeit dynamic diligence complies with the broader concept of meaningful human control, this section will not consider a more specific understanding of this concept. By considering meaningful human control in a narrower fashion, the risk of human error, including that made by experts, would be ignored. To consider that IHL could contain such human error would only thicken the fog of war. Using dynamic diligence, human involvement can be used to best effect, whilst negating the risk of human error.

Interaction Between Human and Machine

The interaction between an AWS and its human operators is vital to ensure its LOAC compliance. To ensure accountability, the interface between the two should be adjusted accordingly. Such adjustments should consider both the chain of command and the AWS' theatre of operations.

[346] Wendell Wallach and Colin Allen, 'Framing Robot Arms Control' (2013) 15 *Ethics and Information Technology* 125, 133.
[347] Michael Horowitz and Paul Scharre, 'Meaningful Human Control in Weapon Systems: A Primer' (Working Paper, Center for a New American Security, March 2015).

To ensure its successful operation, the command structure of an AWS will need to recognise its specialist functionality. It would not be appropriate to treat an AWS like any other infantry weapon, operated with the simplicity of a machine-gun or rocket-launcher. No military unit will be compliant with LOAC if they elect to deploy a non-customised AWS. Due to the specific technical requirements of AWS, their use will require a specialist chain of command.[348]

The reality of modern militaries is such that specialised command structures are commonplace in the operation of complex weaponry. Modern weapons have specific operational and engineering requirements, and mandate a level of commander specialisation unseen in previous centuries. Although 'Crossbow Commands' were not needed in medieval warfare, the modern battlespace has very different requirements. Armoured units, submarines and air power all demand specialist command structures. Indeed, the US also has a dedicated cyber command structure. It would not be unthinkable, therefore, to create a specific AWS command.

AWS commanders will hold important responsibilities. In order to ensure the safe operation of their AWS, they will need to understand machine learning and collaborate with officers and civilians with relevant expertise. In order to safely operate an AWS in the battlespace, its commander, with adequate support staff, should act as a human-on-the-loop.[349] In instances where an AWS has violated LOAC, the on-the-loop commander should be held accountable. Any state which operates an AWS without a committed command structure, and which proceeds to violate LOAC through its use, should present its senior military commanders and civilian leadership as accountable parties.

[348] 'An effect of using increasingly autonomous technologies for targeting is that human actors and technologies are becoming part of a long chain within which decisions made by one link in the chain almost definitely will affect the control or limit the decisions of others in the chain. In short, implementing autonomous technologies will affect the control that human actors further down the chain (i.e., within the targeting process) can exercise. This could result in a shift of responsibilities that, for example, might generate an increase in responsibilities for certain superiors or the developers of systems, but also could result in a lack of accountability if the effects of implementing these technologies are not considered adequately before the technologies are introduced into the process. (This issue is also closely related to the military structure.)' Merel Ekelhof, 'Lifting the Fog of Targeting: Autonomous Weapons and Human Control Through the Lens of Military Targeting' (2018) 71 *Naval War College Review* 23.

[349] Duncan Hollis, 'Setting the Stage: Autonomous Legal Reasoning in International Humanitarian Law' (2016) 5 *Temple International and Comparative Law Journal* 4.

Furthermore, the tactical interface between an AWS and its human operators should be maintained, and able to be adjusted according to the battlespace. Whilst an AWS may be effective when operating fully autonomously in an urban zone, *ex ante* human review of its targeting or real-time human monitoring may be required, on account of the dynamic nature of such environments, and the likely close proximity of civilians.[350] AWS should be able to assess a situation and trigger such a review. Human service personnel should also have the power to override an AWS' machine-learning software. If an AWS did not have such a human interface, and proceeded to violate LOAC, this omission would offer *prima facie* proof of a violation.

Although an AWS needs to interface with human operators, LOAC would not require this interaction if AWS were as effective, or more effective, than their human-operated counterparts. In such circumstances, precaution would not necessitate *ex ante* human authorisation for AWS target selections. In particular, in time-critical scenarios, human approval may not be practicable. Although the US has, amongst other states, required human approval up to now,[351] this practice arguably came about as a result of the lack of any practical alternative. It could be that a state will one day demonstrate the benefits of *post hoc* human target review. In some instances, the time taken to gain human approval, using military lawyers and senior officials, could allow targets to take cover and hide from attack. If this became commonplace, officials could suggest that human review is impractical, and a hindrance to meeting set military objectives.

Furthermore, human involvement in preventing or risking collateral damage is an empirical consideration. Human emotions of anger and fear, alongside cognitive bias, could lead to human targeting errors. Although it is perhaps encouraging to consider human involvement as providing adequate care, this optimistic view could be another indicator of cognitive bias: optimism around the accuracy of human targeting could present an issue, rather than a solution.[352]

[350] Benjamin Wittes and Gabriella Blum, *The Future of Violence: Robots and Germs, Hackers and Drones* (Basic Books, 2015) 32.
[351] Gregory McNeal, 'Targeted Killing and Accountability' (2014) 102 *Georgetown Law Journal* 681, 685.
[352] David Dunning Judith Meyerowitz and Amy Holzberg, 'Ambiguity in Self-Evaluation: The Role of Idiosyncratic Trait Definitions in Self-Serving Assessments of Ability' (1989) 57 (6) *Journal of Personality and Social Psychology* 1082.

Periodic Assessment

AWS assessment should be dynamic. Dynamic assessment indicates that AWS must be continually assessed to make sure that they are, and remain, IHL-compliant and consider the system's tactical experience. Traditionally, commanders should interact with their subordinates and identify any impact caused by enemy contact. Although their role would be more technical, AWS commanders should apply the same level of command responsibility to their interactions with AWS.

Human AWS assessors should review an AWS' performance at regular intervals.[353] In order to assess their performance effectively, assessors should be able to access coded feedback from the system, audio and video recordings, and text responses. AWS should be subject to new tests, determining whether or not the system remains compliant with its scripted parameters, such as its adherence to the LOAC principle of distinction and the coded thresholds for collateral damage imposed by the analysis team. Dynamic AWS assessment should also allow examiners to review the system's software, should evaluations raise any doubt as to the system's compliance with any of its operating parameters.

Further to the above, dynamic assessment will also require a qualified state official to have updated any databases used by the system when selecting targets and deploying on-board munitions. As an example, an AWS could associate a potential target with another person on a terrorist watch list. By making such an association, the system could then increase the conditional probability of that potential target being a member of ISIS. In reality, the likelihood of that assessment being accurate would depend on the accuracy of the system's data inputs. According to US case law, such watch lists contain many pieces of erroneous data, along with some false positives.[354] Furthermore, although individuals are allowed the opportunity to make amends for such mistakes for instance, an updated terrorist screening database, the processes in place to accommodate this are not as fail

[353] US Department of Defense, Defense Science Board, Summer Study on Autonomy (2016) 15; Lieutenant Colonel Christopher Ford, Stockton Center for the Study of International Law, Remarks at the 2016 Informal Meeting of Experts, UN Office in Geneva (2016) 4, at <http:// www.unog.ch/80256EDD006B8954/(httpAssets)/D4FCD1D20DB21431C1257F9B0050B318/$file/2016_LAWS+ MX_presentations_challengestoIHL_fordnotes. pdf.> accessed 25 May 2018.

[354] *Latif v. Holder*, 28 F.Supp.3d 1134 (D.Or.2014); *Abdelfattah v. U.S. Department of Homeland Security*, 893 F.Supp.2d 75, 76 n. 2 (D.D.C.2012).

proof as they should be.[355] In order to facilitate autonomous targeting, data sets must be cleaned on a regular and frequent basis.

Although commanders would not be personally responsible for updating databases, they would hold responsibility for ensuring the currency of their state certification. Arguably, their duty to update such data could be considered a state obligation, in accordance with human rights law. Such law, of course, prohibits arbitrary killing.[356] In cases where a state believes that a commander will input data sets into an AWS for the purposes of informing its targeting decisions, it should conduct regular inspections and certifications of the database, to ensure its currency. Commanders would only be obliged to ensure the currency of the relevant state certification. In the event that an AWS commander was unable to guarantee the currency of such certification, they should immediately halt the targeting operations of the AWS. Dynamic diligence would suggest that any commander who failed to halt an AWS' targeting in such circumstances would have failed in their command duty if that AWS then caused a targeting error.

Dynamic Operational Limits

Alongside the dynamic relationships between AWS and their human operators and periodic evaluations of the systems' performance, AWS will also require dynamic operational limits. Such limits will provide temporal and spatial parameters, along with those for maximum collateral damage. Limits should also consider how easily understood the system's machine learning models are, and whether they can be used singularly, or together with other models.

To reduce the risk of rogue AWS actions, each system should be coded with set temporal and spatial defaults. After a short, specific time period, AWS should be programmed to enter hibernation mode by default. Such a time period might be set between 24 and 96 hours, for example. This hibernation period would allow a human operator to remotely access the system, and, where appropriate, to override this hibernation, and authorise a further operational time

[355] Danielle Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 *Washington Law Review* 1.
[356] *Hassan v. the United Kingdom, 29750/09,* Council of Europe: *European Court of Human Rights, Grand Chamber, Judgment, 16 September 2014,* para 104; *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*, 1996 ICJ 226, 262 (8 July 1996) (noting that 'human rights law applies in armed conflicts').

period. Should no human override be received during the hibernation period, the AWS would then be programmed to power-down which means that stop or shut down the AWS until human intervention was detected. Also, AWS should enter this hibernation state if they were to exceed the spatial limitations opposed upon them, travelling further than the short distance from their launch site specified by their pre-set parameters. As an example, if an AWS identified a senior ISIS leader in Syria as an appropriate target, the hibernation parameters would put the system to sleep if it then travelled beyond a set distance, such as 10 or 15 miles, from its pinpointed target location. As with the temporal limits, human operators could override this default hibernation.

Further to the above limitations, AWS should also be programmed with set limits for collateral damage, depending on their mission and theatre of operations. In a scenario where an AWS is used to target a senior ISIS or Al Qaeda leader, greater collateral damage would be acceptable, and compliant with the LOAC principle of proportionality in order to maintain a direct military advantage. On the other hand, in a scenario whereby a lower-level ISIS figure was to be targeted in an urban zone, the collateral damage ceiling would be much lower. In all modern warfare, US forces operate under the same constraints, ensuring that their actions adhere to standing rules of engagement and those which are mission-specific.[357] Such rules of engagement should also apply to AWS. By doing so, these limits could cause AWS to err on the side of caution and, due to false negatives, fail to strike legitimate targets or civilians directly participating in hostilities. However, by imposing such parameters, even though they may cause an AWS to hesitate when civilian harm is indeed proportionate, the LOAC principles of military necessity and humanity would be adequately protected.

Further, AWS target selection should be easily understood.[358] In the event that a target is mistakenly selected, and compliance with the LOAC principles is questioned, the state operator should be able to clearly demonstrate the AWS' calculation process to a court. In such war crimes tribunals, fact finders would need to assess the reliability of the relevant targeting processes.

[357] Gary Corn, 'Should the Best Offense Ever Be a Good Defense? The Public Authority to Use Force in Military Operations: Recalibrating the Use of Force Rules in the Standing Rules of Engagement' (2016) 49 *Vanderbilt Journal of Transnational Law* 48.
[358] Dustin Lewis, Gabriella Blum, and Naz Modirzadeh, War-Algorithm Accountability 62, (Harvard Law School Program on International Law and Armed Conflict, 2016), available at http://pilac.law.harvard.edu/waa/ 16.

Further, substantive verbal explanations would be the only appropriate method of explaining the system's processes, with its scientific reliability being too subjective and broad to be presented in a clear case to the court.

In order to assess target selection processes, a clear decision-making structure is needed. For example, a decision tree[359] or rule-based model could offer a greater degree of clarity and comprehension to a neural network or opaque machine-learning model. For each of these options to be introduced to a system, the target selection processes contained within AWS would become even more costly. A decision tree alone would not be as accurate as an alternative model. A rule-based approach that blended the results of multiple models would be more complex and time-consuming, and would come at a significant cost. The need for process comprehension, however, justifies the extra cost of such processes.

It is important to consider the interaction between process comprehension and time and dynamic assessment, when target selection justification is situational.[360] Further, it important to remember that in such target selection, neither machine nor human operator has noted a name or personal particulars of a potential target. Consider a scenario whereby a drone's video feed is linked with an AWS' targeting system, and shows potential targets meeting with known low-level ISIS fighters in an Iraqi village. A Bayesian network[361] or decision tree would suggest that such a meeting would increase the likelihood of the potential target being either an ISIS combatant or a civilian who is directly participating in hostilities. That considered, location alone would not necessarily confirm

[359] 'Decision tree models allow you to develop classification systems that predict or classify future observations based on a set of decision rules. If you have data divided into classes that interest you (for example, high- versus low-risk loans, subscribers versus nonsubscribers, voters versus non-voters), you can use your data to build rules that you can use to classify old or new cases with maximum accuracy. For example, you might build a tree that classifies credit risk or purchase intent based on age and other factors.' Available at <https://www.ibm.com/support/knowledgecenter/en/SS3RA7_15.0.0/com.ibm.spss.modeler.help/nodes_treebuilding.htm.> accessed 21 February 2020.

[360] Mark Klamberg, 'Exploiting Legal Thresholds, Fault-Lines and Gaps in the Context of Remote Warfare' in Jens David Ohlin (eds), *Research Handbook on Remote Warfare* (Edward Elgar, 2016) 203.

[361] 'Bayesian networks, also known as belief networks belong to the family of probabilistic graphical models. These graphical structures are used to represent knowledge about an uncertain domain. In particular, each node in the graph represents a random variable, while the edges between the nodes represent probabilistic dependencies among the corresponding random variables. These conditional dependencies in the graph are often estimated by using known statistical and computational methods. Hence, Bayesian Networks combine principles from graph theory, probability theory, computer science, and statistics.' Irad Ben-Gal, 'Bayesian Networks' (2008) *Encyclopedia of Statistics in Quality and Reliability* 1.

that the individuals meeting with the ISIS fighters were also combatants. This co-location could be caused by their attendance at a peaceful event, such as a meeting with tribal elders, or a local wedding.

Furthermore, the initial conditional probability calculation[362] relies heavily on the positive identification of ISIS fighters. This initial calculation can only be assured if dynamic assessment has imposed regular updates of the system databases. Using an interpretable model, the latest database update would also be listed. For older updates, the targeting would be less likely to comply with LOAC.[363]

Even using recent updates, the co-location of the potential targets and ISIS fighters would also be inconclusive. In order to tackle these doubts, and to ensure that conditional probability parameters are LOAC compliant, AWS would require a dynamic temporal limit. The system, much like a remotely-piloted air system, would need to maintain its line-of-sight with the potential target for a longer time period, either increasing or lowering the likelihood of LOAC-compliant targeting. If the co-location of the two parties proved to be short-lived, the conditional probability of a legitimate target would be diminished, as the meeting would then appear to be casual and irrelevant, or, at least, not related to the conflict. However, if the potential target then entered into a vehicle with known ISIS fighters, journeyed with them for over a mile, and spent a further five or six hours with them, the conditional probability of them being a legitimate target would be increased, as an innocent reason would be less probable.[364]

Due to the functionality of drones, enduring reconnaissance missions such as these are achievable. The principle of precaution could, thus, necessitate extra surveillance time, as the death of two

[362] 'The conditional probability of an event B is the probability that the event will occur given the knowledge that an event A has already occurred. This probability is written P(B|A), notation for the probability of B given A. In the case where events A and B are independent (where event A has no effect on the probability of event B), the conditional probability of event B given event A is simply the probability of event B, that is P(B).' Yale University Department of Statistics and Data Science Available at http://www.stat.yale.edu/Courses/1997-98/101/condprob.htm.
[363] Peter Margulies, 'Making Autonomous Weapons Accountable: Command Responsibility for Computer-Guided Lethal Force in Armed Conflicts' in Jens David Ohlin (eds), *Research Handbook on Remote Warfare* (Edward Elgar, 2016) 435.
[364] Peter Margulies, 'Making Autonomous Weapons Accountable: Command Responsibility for Computer-Guided Lethal Force in Armed Conflicts' in Jens David Ohlin (eds), *Research Handbook on Remote Warfare* (Edward Elgar, 2016) 435.

likely civilians in the name of killing two low-level ISIS fighters could be considered excessive. It would, after all, present little military advantage.[365]

Short of a transparent and comprehensible targeting process and the aforementioned dynamic attributes, the scenario presented could imply targeting that would contravene LOAC. Imagine if a war crimes tribunal were to sit, and the prosecution were to present evidence from villagers that confirmed the meeting was a wedding. Suppose that, according to these witnesses, none of the wedding guests were ISIS fighters but, instead, farmers and tradesmen. Suppose, also, that this tribunal could not understand the AWS calculation processes, had no proof that its database of ISIS fighters had been subject to a recent update, and saw no evidence to suggest that the AWS had been afforded extra time to survey the potential targets and their associates. Without such proof, a tribunal could decide that the AWS' targeting decision, in this scenario, had violated LOAC.[366]

Furthermore, consider that human error had caused the AWS to operate in such a way that it did not take any further time to survey its potential target, based on its initial assessment being purely based on co-location. If the system reports were comprehensible, a court could understand this omission of temporal limitations. The AWS commander could then be held accountable for LOAC violations, due to their AWS command responsibility. Should the AWS reports be non-comprehensible, the court could find itself lost in the fog of war. In order to clear the fog, comprehension of AWS systems facilitates the apportioning of accountability.[367]

By adapting laws already in place regarding weapon deployment and employment, it is perfectly possible to make AWS use IHL compliant. The issue of who is accountable for the actions of AWS centres around who has responsibility of command; this responsibility has three strands, which we

[365] Tetyana Krupiy, 'Of Souls, Spirits and Ghosts: Transposing the Application of the Rules of Targeting to Lethal Autonomous Robots' (2016) 16(1) *Melbourne Journal of International Law* 158.
[366] Ian Henderson, Patrick Keane and Josh Liddy, 'Remote and Autonomous Warfare Systems: Precautions in Attack and Individual Accountability' in Jens David Ohlin (eds), *Research Handbook on Remote Warfare* (Edward Elgar, 2016) 358; Peter Margulies, 'The Other Side of Autonomous Weapons: Using Artificial Intelligence to Enhance IHL Compliance' in Ronald Alcala and Eric Talbot Jensen (eds), *The Impact of Emerging Technologies on the Law of Armed Conflict* (Oxford University Press, 2018) 156.
[367] Robin Geiss and Henning Lahmann, 'Autonomous Weapons Systems: A Paradigm Shift for the Law of Armed Conflict' in Jens David Ohlin (eds), *Research Handbook on Remote Warfare* (Edward Elgar, 2016) 392.

shall refer to as dynamic diligence. Dynamic diligence, properly applied, demands extremely high standards. Firstly, there must be a continual dialogue between the machine and its human controllers, with adjustments being made constantly, and the force employing AWS must ensure that the personnel in control of the AWS has the requisite expertise regarding the positives and potential negatives of the system. Secondly, AWS must be continually assessed to make sure that they are, and remain, IHL-compliant. Assessing this factor begins when the weapon is validated in a governmental or military review before the AWS is ever deployed. The assessment must also encompass regular ongoing assessment of the way in which AWS is developing its capacity to learn on the battlefield, making sure that all the decisions being taken by the weapon's software are also compliant with IHL. As part of these assessments, AWS should be regularly updated with the latest information, for example new weaponry it may have to deal with, new forces entering its field operation. Finally, dynamic diligence means that the rules which govern the AWS' operating procedures must have some flexibility, leaning towards being able to interpret its results and make alterations as necessary. Any state that operates proper dynamic diligence towards its AWS can remain IHL-compliant, make sure that if IHL is violated there is clear accountability, and, ideally, make the battlefield safer both for civilians and its own personnel.

Conclusion

The LOAC rules of distinction, precaution, proportionality form the core of IHL. These rules provide a framework within which certain persons are appropriately protected during periods of armed conflict. Any war means or method introduced by state actors should comply with these customary laws. Complimenting the other principles, the principle of humanity dictates that where possible, humanity is taken into account regardless of the decisions made by belligerents and the principle of humanity seeks a balance between humanity and military consideration. I have debated and concluded that, whilst combatants have the right to take the life of another, delegating this power to autonomous machines does not conform to the principle of humanity, and violates the dignity of targeted individuals.

Modern-day conflict typically takes place in densely populated areas. Furthermore, recent armed conflict has seen a much greater civilian involvement. It has become very difficult to discriminate between those who are directly involved in a conflict and those who are not. As such, human

judgements and circumstantial consideration are more important than ever before, and vital when selecting targets in such environments. It is possible that AWS will violate the rule of distinction on a number of counts: the aforementioned nature of modern-day warfare, technological limitations, and the vague IHL definition of a legitimate target that is not clear enough to be programmed into a computer. In terms of the other rules of precaution, military necessity and proportionality, these, too, require human judgment. Thus, AWS lacking 'Meaningful Human Control' should not be permitted, on account of their incompatibility with the LOAC principles of humanity, distinction, precaution, proportionality and military necessity.

Exercising this dynamic diligence to make sure AWS complies with IHL is the opposite of the 'let it run' mode of operation. Dynamic diligence requires that the interactions between the machine and its human controllers are careful and constant, that assessment will be undertaken at frequent regular intervals, and that the parameters of operation are flexible. In terms of its human controllers, there should be a specialised AWS command structure in place, employing personnel who have expertise in the potential and the problems of AWS. This should make it possible for human personnel to intervene at once and overrule any decisions made by AWS; this will be especially important when complex questions arise such as selecting NIAC targets, or choosing targets within built-up environments. Dynamic assessment must regularly review the way in which AWS is learning, and ensure that the data given to the AWS to assist it in target selection, such as a terrorist watch list, is as contemporary as possible. Dynamic diligence also assumes that the ways in which the AWS selects its target will be interpretable.

In some ways, dynamic diligence satisfies the requirement of some observers that a human being should always remain in the loop. Humans cannot simply deploy AWS and leave it to carry on a combat without intervention. However, insisting that a human must always be in the loop may hamper innovative solutions and actually diminish the potential for AWS complying with IHL. Dynamic diligence is effectively allowing humans to have meaningful control of the process, as long as we understand that to be allowing the system to the autonomous whilst making sure that it does not transgress agreed parameters. This is not a simple process. AWS is continually developing and keeping pace with its progress is challenging. The suggestions above allow commanders to take control of complying with IHL in a new way which is nevertheless consonant with the ways

in which the military have conducted themselves for a considerable period. Banning AWS would be to try and pretend that the future will never arrive. Dynamic diligence suggests ways in which the future can be controlled in a way that allows the key principles of IHL to be respected.

Chapter 3 – Can AWS be Deployed in Compliance with the Principle of Proportionality and with Adequate Precautions?

Introduction

This chapter examines the restrictions incorporated in the IHL that influence how AWS can be deployed during armed conflict and the safeguards that must be put in place to protect civilians. The discussion is presented in two sections. The first section provides an overview of what activities are deemed to represent an attack when an autonomous weapon is in use. The provisions outlined in targeting law bind the actions of combatants and their commanders, and the associated attacks are regulated by the legal obligations. There is a requirement to understand what the term attack represents when an assault is launched by a weapon that is operating autonomously or with reduced human intervention. The second section presents an example of a targeting process which examines whether machine learning and artificial intelligence technology have the potential to distinguish between legitimate military targets, military objectives, combatants, and civilians directly participating in hostilities and make adequate precautionary considerations of an operation with the possibility of translating proportionality principles into computer programs.

Within the framework of international law, conflict is governed by two distinct legal bodies: *jus ad bellum* and *jus in bello*. *Jus ad bellum* dictates how and when a State can use force within its national policy. These legal bodies address a number of matters, including a ban on State use of force and any relevant exceptions. In particular, they refer to the right of self-defence and UN Security Council authorisation or mandates.[368] *Jus in bello*, however, governs the use of force by combatants and militaries, as well as the legitimacy of their targets.

According to international humanitarian law, an attack is a specific type of military action. As defined by Article 49(1) of the 1977 Additional Protocol I to the Geneva Conventions, an attack is any violent act against an adversary, and includes offensive and defensive actions. The term attack is, in itself, a neutral term as, while some are legal, others are indeed illegal. Attacks can be deemed legal or illegal based on their object, or on their nature. Despite being a neutral term, the

[368] U.N. Charter, arts. 2(4), 42 & 51.

concept of an attack represents a central component of international humanitarian law; many of the key restrictions and prohibitions enforced by this law apply only when an action is deemed to be an attack. As such, this section will analyse autonomous attacks, within the framework of *jus in bello*.

There are two different types of weapons. First, weapons with an instantaneous effect such as rifles. Second, delayed action weapons such as mines, cyber and autonomous weapon systems. The major difference between these two different types of weapons is the occurrence time of an attack. The current author propounds that delayed action weapons and weapons with an instantaneous effect can be reconciled with the point at which a specific target is defined. The question that is of relevance to this chapter is: Can this concept be reasonably applied to AWS? Or, in light of the fact that AWS can involve both instantaneous and delayed action weapons, can a meaningful analogy be drawn between AWS and other weapon forms? Or is there a need to develop a discrete category with unique rules for weapon systems that incorporate autonomous abilities?

This chapter also explores clarification that distinction/proportionality decisions are taken by commanders/weapons operators, not AWS, and that where possible these decisions should be made in advance, when the weapons are deployed or even earlier. An interpretation of the way that IHL can be applied to AWS, detailing the information commanders require and the questions they should usually pose prior to and in the course of deployment. A description of real-world deployment scenarios, from simple to extremely complicated, looking at those elements of MHC standards that must be observed in order to be compliant with IHL norms. A restatement of the central nature of the ‘constant care’ obligations and their implications for the precautionary principles of IHL, and how this works with AWS. A consideration of those scenarios during armed conflict in which human rights norms become more significant, and so more contemporary human decision-making and control is required, even in some cases demanding the shutdown of the AWS or a remote pilot taking over.

Autonomous Attacks

The previous chapter made extensive reference to the use of AWS to launch attacks. Attacks are 'a unit of legal management and tactical action',[369] a method by which a given objective can be achieved; i.e., a physical assault represents a means by which the military's requirements can be achieved and the legal framework under which this attack is launched represents the means by which the humanitarian objectives of IHL can be achieved. The central values of IHL in terms of proportionality and distinction are essentially exemplified in the rules that oversee the methods by which these attacks are performed.

By asserting a set of legal requirements that govern the process by which attacks are planned, prepared for, and launched, the IHL aims to achieve a humanitarian objective of reducing the consequences of armed warfare. The parties that take part in armed conflict must demonstrate compliance with a vast array of requirements related to the planning and implementation of attacks, who or what they are directed at, and the process by which they are conducted. Within their planning processes, attacking parties are required to demonstrate adherence to a set of legal norms that span both customary and conventional sources of international law to ensure that the attack is limited to a military target, the method by which the attack is launched is legitimate, and that the risks to civilians and civilian entities are kept to a minimum and are proportional to the military advantage that can be gained from the attack.[370] Attackers who fail to meet these obligations in the

[369] Richard Moyes, (Notes, CCW Meeting of Experts on LAWS: Towards a Working Definition of LAWS, April 2016) 1.

[370] Article 48 of the 1977 Additional Protocol I provides: '[T]he Parties to the conflict shall at all times distinguish between the civilian population and combatants.' Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), Geneva, 8 June 1977, Article 48. Article 48 was adopted by consensus. CDDH, Official Records, Vol. VI, CDDH/SR.41, 26 May 1977, p. 161; Article 51(5)(b) of the 1977 Additional Protocol I prohibits 'an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.' Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), Geneva, 8 June 1977, Article 51(5)(b). Article 51 was adopted by 77 votes in favour, one against and 16 abstentions. CDDH, Official Records, Vol. VI, CDDH/SR.41, 26 May 1977,163; Article 57(1) of the 1977 Additional Protocol I states: 'In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects.' Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), Geneva, 8 June 1977, Article 57(1). Article 57 was adopted by 90 votes in favour, none against and 4 abstentions. CDDH, Official Records, Vol. VI, CDDH/SR.42, 27 May 1977, 211.

process of launching an attack violate the law. Operations that are not considered to amount to attacks are not governed by such stringent obligations.[371]

It is critical that all parties have a comprehensive understanding of what represents an attack and the conduct they need to exhibit when an attack is planned or implemented. In addition, if any major modification in terms of the type and nature of the weapons that will be used in the attacks or the methods by which they are used is planned, it is imperative that the appropriate laws are consulted to ensure such changes remain within the realms of the legislation governing attacks and the use of weapons.

The introduction of AWS will present some complications that entail it will be necessary to re-examine what represents an attack.

The primary challenge can be traced back to the inherent purpose, and probable outcome, of enhancing the autonomy of weapons systems: To reduce the extent to which human beings are directly involved, both causally and physically, in violent acts. Creating a distance between humans and the act of violence is likely to be achieved in at least three ways:

1. By extending the deployments with limited or zero opportunity for human intervention, during the course of which the conditions that lead to attacks may evolve. This could include deployments in which agents cannot be sure whether targets will be attacked or not; for example, in situations in which AWS are deployed as a mechanism of defence.
2. Due to an array of dissimilar, potentially unanticipated, conflict situations during a specific deployment.
3. As a result of different AWS, or components of a network of AWS, directly communicating with each other in the absence of a human decision-maker.

Activities that are specifically designed to distance humans from warfare by providing weapons systems with the ability to choose and attack targets without any human intervention muddies the

[371] Michael Schmitt, 'Fault Lines in the Law of Attack' in Susan Breau and Agnieszka Jachec-Neale (eds), *Testing the Boundaries of International Humanitarian Law* (British Institute of International and Comparative Law, 2006) 277.

waters of what existing legal frameworks consider to represent an attack.[372] For instance, how the attack definition is applicable or relevant to delayed action weapons which activated sometime after the last human involvement. Major examples are cyber weapons, mines and autonomous weapon systems. This then makes it difficult to determine what legal obligations are related to such an attack.

One fundamental motivation that drives decisions to enhance the autonomy of weapon systems is to exploit the 'potentially unlimited persistent capabilities' of AWS.[373] For example, a given State could attempt to combine ISR[374] and strike capabilities in a single platform[375] that has the ability to linger in the proximity of enemy operations in a given area of land, water, air, sea, or cyberspace for extended periods. Systems of this nature would have the ability to immediately respond to threats as they emerge without the need for significant human intervention, if any at all. Using such a platform, it may be possible for States to respond more rapidly to threats, reduce the risk to personnel, and decrease costs. As such, it is highly likely that, as the functionality and capabilities of AWS evolve, human operators will express increasing interest in deploying such systems in their defensive and offensive efforts.

According to API Article 57(2)(a)(iii), there is a requirement for attack planners and associated personnel to perform a proportionality assessment in advance of each attack. However, the way in which the principle of proportionality will apply to AWS that are in use over a prolonged period of time with very little human intervention—for example, a UAV that is positioned in enemy airspace or an autonomous UUV[376] that patrols an area of land that is under enemy control—becomes murky. Planners may have no way of knowing in advance what, if any, enemy targets will emerge and, in the event such targets are encountered, in what situations it will be appropriate to attack them. In light of this, should every deployment of AWS represent some form of attack

[372] 'There are many elements that make a human being understand what is/is not a legitimate target, and those factors must be reproduced in a computer program.' Marco Sassoli, 'Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified' (2014) 90 *International Law Studies / Naval War College* 327.
[373] Defense Science Board, 'The Role of Autonomy in DoD Systems' (Task Force Report, US Department of Defense, July 2012) 1.
[374] ISR (Intelligence, surveillance and reconnaissance)
[375] Defense Science Board, 'The Role of Autonomy in DoD Systems' (Task Force Report, US Department of Defense, July 2012) 15.
[376] UUV (Unmanned underwater vehicle)

that requires a proportionality assessment? If so, it is only possible to perform such an assessment in advance of any enemy encounter. As such, is it possible for operators and developers to adequately assess the proportionality? Would an attempt to do so achieve the fundamental objective of the law, which is to ensure that an adequate balance between military necessity and humanitarian considerations is maintained? Could each incidence of violence that takes place during a prolonged deployment be viewed as a separate attack? Would this entail that AWS represent entities that have the responsibility to 'plan or decide upon an attack'? If that were to be the case, the obligations related to the need for the attack to be borne by humans would not be met. Does this mean that there is a need to perform a proportionality assessment for every encounter with an enemy? If so, would some degree of human intervention be required, or would there be a technical prerequisite for AWS to possess the functionality to perform a proportionality assessment without human intervention?

This section commences with an overview of the legal obligations associated with planning and launching an attack, and examines the existing understanding of what represents an attack under IHL. It then progresses to consider how the law can potentially be applied to weapons systems that incorporate some degree of autonomy.

How an Attack is Defined

Despite the prominent role that the term attack plays within existing international law, the definition that is applied within the contemporary setting can be traced back as far as the mid-1950s. The rules related to the methods and means of warfare were first set out in the Hague Regulations of 1899[377] and 1907.[378] Two of these provisions unequivocally reference attacks: Article 25 forbids '[t]he attack or bombardment, by whatever means, of towns, villages, dwellings, or buildings which are undefended' and Article 26 mandates that '[t]he officer in command of an attacking force must, before commencing a bombardment, except in cases of assault, do all in his power to warn the authorities.' While the regulations do not formally delineate what represents an attack, they do highlight that an attack represents the use of violence against an adversary. Significant developments in the means of warfare[379] that emerged since the early Hague

[377] Hague Convention 1899 annex s II.
[378] Hague Convention 1907 annex s II.
[379] Principally developments relating to missile technology, artillery and military airpower.

Regulations undermined compliance with ideological conflict in the Cold War these treaties embodied and major changes in military operations were observed that ultimately resulted in large-scale civilian fatalities and losses during the conflicts of the twentieth century. During the 1949 Diplomatic Conference, which led to the creation of the Fourth Geneva Convention,[380] the Soviet delegation made a move to pass a Draft Resolution that outlawed certain weapons; however, the Conference concluded that it lacked the required authority to establish directives related to the 'the means of war, the methods of warfare, or the weapons of war';[381] as such, that particular task was delegated to the United Nations. As a direct result, not one of the four Geneva Conventions of 1949 presents a formal definition of the word attack. However, the use of the word within these Conventions mirrors how it is applied and interpreted in the Hague Regulations.

The 'Draft Rules for the Limitation of the Dangers Incurred by the Civilian Population in Time of War'[382] were introduced by the International Committee of the Red Cross in 1956 in a bid to close the gap between the existing formal rules that governed the means and methods of conflict and the reality of State practices. Article 3 of those draft rules specifies the following:

'[t]he present rules shall apply to acts of violence committed against the adverse Party by force of arms, whether in defence or offence. Such acts shall be referred to hereafter as attacks.'

This rule represents the first formal definition of what signifies an attack in modern IHL. However, even though the draft rules were approved by the 19th International Conference of the Red Cross in New Delhi in 1957, governments did not consequently act on them. Later, during the negotiations that contributed to the formation of the 1977 Additional Protocols to the Geneva Conventions, a definition of attack was once again presented in Article 44(2) of the Draft Additional Protocol I to the Geneva Conventions of 1949:

---

[380] *Geneva Convention Relative to the Protection of Civilian Persons in Time of War*, opened for signature 12 August 1949, 75 UNTS 287 (entered into force 21 October 1950) ('*GCIV*').

[381] *Final Record of the Diplomatic Conference Convened by the Swiss Federal Council for the Establishment of International Conventions for the Protection of War Victims and Held at Geneva from April 21*st *to August 12*th, *1949* (Federal Political Department, Berne) vol. IIB, 498.

[382] *Draft Rules for the Limitation of the Dangers Incurred by the Civilian Population in Time of War* (International Committee of the Red Cross, 1956) <https://www.icrc.org/ihl/INTRO/420?OpenDocument>.

'These provisions apply to acts of violence committed against the adversary, whether in defence or offence. Such acts are referred to hereafter as attacks.'[383]

and in the proceedings of each part of the 'Conference of Government Experts on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts' that was held in Geneva in 1971 and 1972:
'This word attack is used here in its purely military and technical sense; it means acts of violence perpetrated against the adversary, either defensively or offensively, whatever may be the means or arms employed.'[384]

'... the ICRC expert specified that the concept of attack should be understood here in a military and technical sense and not in a politico-legal sense; ...'[385]

In the aftermath of these events, the definition of attack that is in wide use today appeared as Article 49(1) of API:[386]

'Attacks means acts of violence against the adversary, whether in offence or in defence.'

It is worth examining each of these three elements of the API definition in more depth in light of the fact that, although the definition supports the enforcement of the required standards, ensuring that the objectives of API are achieved depends, to a certain degree, on the reinterpretation of the meanings of the terms that were originally contained within it. Because the definition of attack is not appropriately adapted to delayed action weapons such as mines, autonomous cyber weapons

[383] International Committee of the Red Cross, *Draft Additional Protocols to the Geneva Conventions of August 12, 1949 – Commentary* (1973) 54.
[384] International Committee of the Red Cross, *Conference of Government Experts on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts, 24 May -12 June, 1971* (1971) vol. III: Protection of the Civilian Population Against Dangers of Hostilities, 21.
[385] International Committee of the Red Cross, *Conference of Government Experts on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts, Second Session, 3 May -3 June 1972 – Report on the Work of the Conference* (1972) vol. I, 148 [3.147].
[386] Michael Schmitt, Charles Garraway, and Yoram Dinstein, *The Manual on the Law of Non-International Armed Conflict with Commentary*, International Institute of Humanitarian Law available at http://www.iihl.org/iihl/Documents/The%20Manual%20on%20the%20Law%20of%20NIAC.pdf 7.

which have a significant difference from kinetic weapons, for instance, both of them be activated sometime after the last human involvement.

Acts of Violence

Within the definition presented in API, violence refers to a physical act;[387] that is, it describes the use of some form of force or influence that can kill or cause damage. Similarly, HPCR Manual on International Law indicates that activities such as propaganda, intelligence gathering which do not cause in damage cannot be accepted as an attack.[388]For example, the use of kinetic weapons, such as missiles and guns, during combat represents a viable and acceptable form of attack in some situations, as too does the use of biological, chemical, or radiological agents.[389] Strategies, such as enforcing embargoes or proliferating propaganda, can indirectly result in an adversary coming to harm; however, they do not directly inflict harm. As such, they do not represent acts of violence or attacks.

Where a fighter performs an action that directly results in violence, such as firing a missile or gun, this represents an attack. This simple correlation was no doubt what the individuals who negotiated the terms of API had in mind when it was developed. However, the means and methods of combat have significantly changed since API came into force and this entails there is a need to extend the definition and scope of what represents an act of violence. Specifically, in the contemporary landscape, although the requirement remains for there to be a direct link between the act that is performed and the resulting violence, such violence may not be part of, or even a direct outcome of, the act. In some scenarios, the violence could take the form of a second or higher-order effect; for example, in the case of cyber-attacks, the very nature of the target systems entails that the attack may be perpetrated over an extended period of time via a series of stages:

'The crux of the notion lies in the effects that are caused. Restated, the consequences of an operation, not its nature, are what generally determine the scope of the term attack; violence must

[387] Michael Bothe, Karl Partsch and Waldemar Solf, *New Rules for Victims of Armed Conflicts* (Martinus Nijhoff, 2013) 329.
[388] The Program on Humanitarian Policy and Conflict Research HPCR Manual on International Law Applicable to Air and Missile Warfare (2013) 12.
[389] *Prosecutor v Tadić (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction)* (International Criminal Tribunal for the Former Yugoslavia, Appeals Chamber, Case No IT-94-1, 2 October 1995) [120], [124].

be considered in the sense of violent consequences and is not limited to violent acts. For instance, a cyber-operation that alters the running of a SCADA [Supervisory Control and Data Acquisition] system controlling an electrical grid and results in a fire qualifies. Since the consequences are destructive, the operation is an attack.'[390]

The extension outlined above seems to be crucial to accomplish the objective and goal of API; the wording that was negotiated in Article 49(1) did not consider the emergence of technologies through which combatants can ultimately achieve the end characteristic of an attack, causing harm, while not directly engaging in what API considers to an act of violence.

It is also important to note that the deliberate violent outcome that would represent a form of attack 'is not limited to effects on the targeted cyber system. Rather, it encompasses any reasonably foreseeable consequential damage, destruction, injury, or death.'[391] According to this provision, any unintentional, yet conceivable, consequent harm that is caused to civilians or civilian objects would represent collateral damage. This entails that an action can be considered to represent an attack even if it does not directly result in physical damage. For example, if the actions were performed with the intention of causing harm, but are unsuccessful, according to the IHL, they still represent an act of violence and, therefore, an attack.[392] The factor that is of interest is the intent to cause harm through violence, regardless of whether such violence is a direct outcome of the act or a consequence that will come to fruition at a later time.

Scale

While the laws do not explicitly specify what scale the action needs to be performed on for it to represent an attack, the Commentary to the Draft Additional Protocols highlights the following: 'it

[390] Michael Schmitt (ed.), NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017) 415-6 [3] (rule 92).
[391] Michael Schmitt (ed.), NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017) 107 [5].
[392] Michael Schmitt (ed.), NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017) 110 [15]; 'The term attack includes both operations that actually result in violent effects, and those which were intended to but failed. For instance, an aircraft which intends to bomb a target but is unsuccessful because its weapon system fails to release due to mechanical failure, has nevertheless conducted an attack. Similarly, enemy defences may effectively foil an attack and therefore an attack may not be completed; an incomplete attack, still counts as an attack.' The Program on Humanitarian Policy and Conflict Research HPCR Manual on International Law Applicable to Air and Missile Warfare (2013)12

is related to only one specific military operation, limited in space and time.'[393] According to this perspective, military operations represent 'the movements, manoeuvres and actions of any sort, carried out by the armed forces with a view to combat.'[394] With regards to AWS, it is noteworthy that an individual attack is considered to overlap with a distinct military operation; an attack 'refers simply to the use of armed force to carry out a military operation at the beginning or during the course of armed conflict.'[395] Similarly, 'The author of an attack is he who, whatever his position may be at the outbreak of hostilities, starts a military operation involving the use of arms.'[396]

The acts that represent acts of violence are understood as deeds that can be directly attributed to a participant in the conflict; for example, a State, via its armed forces. The participants in the conflict may engage in single or multiple acts of violence. There are some textual references in API that indicate there is a requirement for some level of planning and co-ordination across the governing and military hierarchy; for example, Article 57(2)(a) asserts '[t]hose who plan or decide upon an attack.' Elsewhere, there is also a statement that highlights how the definition does not exclude 'acts of violence by an individual combatant such as a sniper acting alone, or a single bomber aircraft.'[397] However, that is not to say that every act of violence that is carried out by an individual fighter constitutes an attack in its own right;[398] rather, it is the coordinated acts of violence that are executed as part of a larger operation that aims to achieve a shared objective that represents an attack.

[393] International Committee of the Red Cross, *Draft Additional Protocols to the Geneva Conventions of August 12, 1949 – Commentary* (1973) 54.
[394]Bruno Zimmermann, 'Protocol I – Article 3 – Beginning and End of Application' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 65, 67 [152].
[395] Claude Pilloud and Jean Pictet, 'Protocol I – Article 49 – Definition of Attacks and Scope of Application' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff,1987) 601, 603 [1882].
[396] International Committee of the Red Cross, *Draft Additional Protocols to the Geneva Conventions of August 12, 1949 – Commentary* (1973) 54.
[397] Michael Bothe, Karl Partsch and Waldemar Solf, *New Rules for Victims of Armed Conflicts* (Martinus Nijhoff, 2013) 329.
[398] William Fenrick, 'The Rule of Proportionality and Protocol I in Conventional Warfare' (1982) 98 *Military Law Review* 91, 101–2.

The plural use of the word objectives that appears in API Article 57(2)(a)(i)[399] emphasises how a single attack can be linked to multiple objectives if such objectives are underpinned 'by a specific military formation engaged in a specific military operation.'[400]

This leads to the question of whether the scale of a single attack has an upper bound. For example, for the purposes of API, could all of the single acts of violence that are perpetrated during the capture of a location that was previously under the control of an enemy be treated as a single attack? The perspective that an attack relates to 'one specific military operation' indicates that some form of upper limit is in existence; however, this upper limit has not been clearly delineated. That said, it is possible to identify a *de facto* upper limit for an attack that complies with API in accordance with the relevant legal obligations.

An attack represents the military action for which there is a requirement to perform proportionality assessments and take the additional precautions outlined in Article 57. If the State that wishes to launch an attack is unable to meet these requirements, it cannot legally proceed according to API. However, a fundamental issue concerns the fact that the capacity to perform a proportionality assessment and take additional precautions is subjective, situational, depends on the resources and technologies that the party that is launching the attack has access to, and is contingent on the adversary's actions.[401] Theoretically speaking, if an attacker possesses the ability to sufficiently forecast the output of an aggressive action that is performed as part of a major operation in adequate detail to identify the civilian and/or military status of all potential targets and, therefore, develop a precise proportionality assessment, there does not seem to be any *prima facie* impediment to viewing the operation in its entirety as a single attack for the purposes of API.

[399] William Fenrick, 'The Rule of Proportionality and Protocol I in Conventional Warfare' (1982) 98 *Military Law Review* 91, 102.
[400] Michael Bothe, Karl Partsch and Waldemar Solf, *New Rules for Victims of Armed Conflicts* (Martinus Nijhoff, 2013) 329.
[401] 'It is generally agreed that in this context, feasible means that which is practicable or practically possible, taking into account all circumstances prevailing at the time, including humanitarian and military considerations.' International Humanitarian Law Research Initiative, HPCR Manual on International Law Applicable to Air and Missile Warfare (2009), online: Program on Humanitarian Policy and Conflict Research at Harvard University ('HPCR Manual') rule 1.q, <http://ihlresearch.org/amw/HPCR%20Manual.pdf> accessed 2 December 2018.

Often, air-launched attacks are performed by a collection of military aircraft and, as such, it would not be appropriate to examine the impact of individual sorties in isolation. Rather, it would be most appropriate to assess the impact of each mission in its entirety. When considering military advantage in terms of an entire attack, other factors should also be examined. Consider, for example, a series of attacks on multiple bridges across the same river, where these bridges are close to one another. Whilst an initial bridge attack might only offer a small military advantage, with the remaining bridges still being available to the enemy, significant military advantage would only be gained when subsequent bridges were destroyed.

The notion of an entire attack should not be confused with that of an entire armed conflict. The term could, however, relate to a sizeable air campaign. For instance, a series of air-launched attacks could target a group of military objectives within one geographical zone, in advance of a military operation elsewhere. Such tactics could be used to fool enemy forces about the true location of planned missions. Whilst any collateral damage to civilian objects or individuals might be considered disproportionate in terms of the specific advantage gained from those attacks, it should, instead, be assessed in terms of the value of this decoy and its impact on wider military operations.[402]

Severity

As is the case with the scale of the attack, API does not explicitly define the severity of the intended harm needed for an act to qualify as an attack. However, considering the means and methods of warfare that the armed forces had access to at the time, it is doubtful that there was a significant amount of disagreement about the type of harm that was to be governed by the regulation. According to a number of articles, the focus of API is on comparatively severe harm, such as 'loss of civilian life',[403] 'severe losses among the civilian population',[404] 'widespread, long-term and severe damage to the natural environment',[405] etc. However, additional articles use less specific terms; for example, 'injury to civilians, damage to civilian objects.'[406]

[402] Program on Humanitarian Policy and Conflict Research Manual on International Law - Applicable to Air and Missile Warfare rule 14.
[403] API art 57.
[404] API art 56(1).
[405] API art 35(3).
[406] API art 51(5)(b).

It may be deduced that there is a lower level of intended physical harm, below which an operation does not constitute an attack; however, there is no clear definition available as to what this lower threshold is. The issue is of particular relevance within the context of cyber-attacks, which typically cause harm that is not of the traditional type (kinetic, chemical, etc.) and are more likely to result in the obliteration of important data or equipment, which leads to further harm of a different form. The overall consensus is that '*de minimis* damage or destruction does not meet the threshold of harm',[407] although the loss of life or serious injury to people, ruin of buildings and monuments, and similar levels of harm do pass the harm threshold. However, the exact point at which the lower threshold is passed is not explicitly delineated. A moderate view that is suitable for the analysis presented in this thesis is that an operation that has a real potential to kill or cause serious injury to at least one individual and/or result in major destruction or damage to a given target should be perceived to represent an attack.[408] We accept that this view as a moderate one because *the Tallinn Manual* states that a cyber-attack 'is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.'[409] The restriction in this rule does not exclude cyber operations which can be applied to autonomous cyber-attacks as customary international law.

Against the Adversary

This element of the definition was the only aspect that stimulated a major discussion among members of the Drafting Committee. Some of the attendees argued that restricting the concept of an attack to something that resulted in violence against the adversary was contradictory to this element of API, which aims to safeguard civilians against harm that could result from the attacks, including the civilians belonging to the State that levied the attack.[410] While the words were

[407] Michael Schmitt (ed.), NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017) 416 [4] (rule 92).
[408] Michael Schmitt (ed.), NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017) 419 rule 92 [16].
[409] Tallinn Manual, Rule 30.
[410]Claude Pilloud and Jean Pictet, 'Protocol I – Article 49 – Definition of Attacks and Scope of Application' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 602 [1877]; 'Summary Record of the Eleventh Meeting (CDDH/III/SR.11)' in *Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts Geneva (1974–1977)* (1978) vol. 14, 85–6.

retained in this form, additional articles in Part IV of API elucidate on protection for the civilian population.

Understandably, States, practitioners, and judicial bodies commonly rely on the simple definition of the word attack when referencing violence that is directed at civilians and civilian targets, and it is common for legal discussion to focus on questions related to the legitimacy of the target that was attacked. It is certainly arguable that the inclusion of the provision against the adversary in the definition of an attack destabilises such a consideration: If the action does not target an adversary, is it not an attack?

Given that the word attack is the legal concept to which the conditions of proportionality and superfluous injury/unnecessary suffering relate, the omission of attacks against civilians seems reasonable, as these concepts would only become an issue if it is legal to attack the target of the operation. However, prevalent practice depends on the concept of attack that considers the chance that such an attack may be waged against targets other than the enemy.[411]

Whether in Offence or in Defence

This statement elucidates on the fact that the definition refers to an attack as 'use of armed force'[412] or 'combat action',[413] without explicitly referring aggression, the initial application of force, or accountability for starting a conflict;[414] violent actions that were performed with the intention of deterring an attacker are as much attacks as the hostile action that motivated them. Many scholars have highlighted how, in this regard, the definition of attack that is presented in API deviates from

[411] Michael Schmitt (ed.), NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017) 417 [7] (rule 92).
[412] Claude Pilloud and Jean Pictet, 'Protocol I – Article 49 – Definition of Attacks and Scope of Application' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 603 [1882].
[413] Claude Pilloud and Jean Pictet, 'Protocol I – Article 49 – Definition of Attacks and Scope of Application' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 603 [1880].
[414] Claude Pilloud and Jean Pictet, 'Protocol I – Article 49 – Definition of Attacks and Scope of Application' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 603 [1882].

the largely accepted dictionary definition and that presented in the majority of military manuals;[415] however, there is no solid evidence to suggest that this deviation causes difficulties.[416]

Application to Delayed-Action Weapons

The negotiations that resulted in the wording way of API were predominantly uncontentious and by no means prompted a major form of controversy. However, the inclusion of the phrase against the adversary in API did stimulate some dispute at the time of the negotiation. However, since the treaty was finalised, it has become increasingly clear that the definition cannot be readily applied to attacks that involve delayed-action weapons; i.e., weapons that can be used a significant amount of time after humans were last involved. As a result of these issues, the originally simple API definition has been extended.

Mines

During an International Congress in Lausanne in 1982, the International Society of Military Law and the Laws of War, asked attendees from a range of representative nations a series of questions related to API. One such question was 'What is, in your armed forces, the usual meaning of the term attack?'[417] The answers the delegates gave to this question indicated that there was no major inconsistency between their views on this issue, with them all providing responses that were aligned with the API definition, although with more of a focus on aggressive action. The response provided by the representative from the UK was typical of that of the other delegates:

'To attack in common military parlance means, to take offensive military action, but it can include opening fire from a defensive position. In this sense the definition in Protocol I does not appear to cause any difficulty.'[418]

However, this particular response was followed by a further statement:

---

[415] Claude Pilloud and Jean Pictet, 'Protocol I – Article 49 – Definition of Attacks and Scope of Application' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 603 [1879]–[1880].
[416] William Parks, 'Air War and the Law of War' (1990) 32 *Air Force Law Review* 1, 115–6.
[417] International Society of Military Law and the Laws of War, *Armed Forces and the Development of the Law of War (Ninth International Congress, Lausanne, 2–6 September 1982)* (1982) 58.
[418] International Society of Military Law and the Laws of War, *Armed Forces and the Development of the Law of War (Ninth International Congress, Lausanne, 2–6 September 1982)* (1982) 207.

'Questions have been raised, however, as to what stage in a mine-laying operation amounts to an attack. Is it when the mine is laid, or when it is armed, when a person is endangered by the mine or when it finally explodes? From a purely legal point of view, the answer must be that the attack occurs when a person is immediately endangered by a mine.'[419]

This remark is useful when attempting to delineate the point at which an attack takes place when there is a significant period of time between the last act performed by the attacking force and the point at which violence is inflicted on the target. As such, it raises some important questions. For example, the delegate did not offer any clarification as to the exact conditions in which a civilian is 'immediately endangered', despite the failure to secure consensus among the delegates.[420] Is a civilian 'immediately endangered' at the point at which they surpass a threshold probability of being the victim of a violent action? Or when an act of violence becomes unavoidable? Is the risk to the victim connected to their temporal or physical proximity to the point at which the mine explodes? Although the ICRC later described how the view that had been shared by the UK delegate was representative of the 'general feeling' of the delegates as a collective whole,[421] no further elaboration was provided.

Despite this lack of elaboration, the response the UK delegate shared at the conference is useful for the purposes of this dissertation because it implies that the conditions in which an operation represents an attack can be fulfilled long after any type of human involvement. When provided with a series of alternatives, which included the alternative to place the attack at the point at which the mine was physically placed (i.e., the last point of human involvement), the delegates were of the opinion that the placement of the mine only amounted to an attack at the point someone encountered an immediate risk of violence. It is also worth noting that a mine attack was stated to

[419] International Society of Military Law and the Laws of War, *Armed Forces and the Development of the Law of War (Ninth International Congress, Lausanne, 2–6 September 1982)* (1982) 207–8.
[420]International Society of Military Law and the Laws of War, Armed Forces and the Development of the Law of War (Ninth International Congress, Lausanne, 2–6 September 1982) (1982) 341 (India); Elmar Rauch, 'Intervention' (1983) 22 *Military Law and Law of War Review* 291, 293 (Germany).
[421] Claude Pilloud and Jean Pictet, 'Protocol I – Article 49 – Definition of Attacks and Scope of Application' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 603 [1881].

have been launched at the time the mine was placed, before any violence resulted from the explosion of that mine.

It is possible to reconcile this notion of a mine attack with the API definition by observing that an operation is considered to be tantamount to an attack if the act of violence is specifically focused on a target. It is possible to distinguish between the target of an attack and other individuals who may be in the vicinity by considering where the specific focus of the weapon was. In advance of someone being in the vicinity of a mine and, therefore, at risk of being harmed by it, no single individual can viably be considered to be the focal point of the attack. To put it an alternative way, an attack involving an explosive projectile results from the projectile moving to an individual, while an attack that is levied via a static explosive takes place when the individual moves to the bomb. The target's identity is a prime consideration in the legal definition of what represents an attack because, in advance of the emergence of the focal point, it isn't feasible to evaluate the extent to which the attacker has complied with obligations related to proportionality, distinction, and other factors that are of relevance to the attack in question.

Cyberattacks

In more recent years, the increased threat of armed conflict being conducted via technology and computer systems has incited a further analysis of the actions that represent an attack according to the provisions of API. While the role computer systems play in attacks and violent acts remains a subject of significant debate, *the Tallinn Manual on the International Law Applicable to Cyber Warfare*[422] and, later, *the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*[423] have played a significant role in adding clarity to the legal provisions related to cyberattacks. Additionally, there are some states such as the UK, France, China and USA have publicly available national security doctrines which applicable to cyberspace. These national security doctrines refer to customary international law principles such as *the Tallinn Manuals*.[424]

[422] Michael Schmitt (ed.), NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013).
[423] Michael Schmitt (ed.), NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017) 415-6 [3] (rule 92).
[424] See, e.g., The White House International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (May 2011), available at <https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>; The DoD Cyber Strategy (April 2015), available at <https://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_

The International Group of Experts that directly contributed to these documents based the concepts on API's definition of attack and the prevailing view of the way in which this definition applies to mine attacks. However, they extended the fundamental concepts to the unique setting of computer networks and operations:

'The general feeling of the [API] negotiators was that there is an attack whenever a person is directly endangered by a mine laid. By analogy, the introduction of malware or production-level defects that are either time-delayed or activate on the occurrence of a particular event is an attack when the intended consequences meet the requisite threshold of harm. For the majority, this is so irrespective of whether they are activated."[425]

The analogy that was drawn between malware and mine attacks was certainly not perfect. After presenting this comparison, *Tallinn Manual 2.0* progressed to assert:

'An attack that is successfully intercepted and does not result in actual harm is still an attack under the law of armed conflict. Thus, a cyber-operation that has been defeated by passive cyber defences such as firewalls, anti-virus software, and intrusion detection or prevention systems nevertheless still qualifies as an attack if, absent such defences, it would have been likely to cause the requisite consequences."[426]

Virus protection, intrusion prevention, and firewall systems predominantly operate on the network border. If they are successful in their objectives, the malware does not infiltrate the target system; as such, the failure in this regard would be comparable to failing to place a mine. By considering a failed attempt to install malware on a system to represent an attack, *the Tallinn Manual* suggests that, at least in the case of some cyber-attacks, a more suitable analogy is that of a missile that is

for_web.pdf>; China's International Strategy of Cooperation on Cyberspace (Mar. 2017), available at http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm; Secrétariat Général de la Défense et de la Sécurité Nationale, Strategic Review of Cyber Defense (February 2018), available at <http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf>; The National Cyber Security Strategy 2016 to 2021 (Nov. 1, 2016), available at <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021> accessed 18 February 2020.

[425] Michael Schmitt (ed.), NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017) 419 rule 92 [16].

[426] Michael Schmitt (ed.), NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017) 419 rule 92 [17].

launched but is intercepted by a missile defence system. The attack was launched, even though it was unsuccessful.

There is also an implicit assumption in *the Tallinn Manual* that the system on which the attackers attempt to install the malware is the final intended target of the attack. This is not necessarily true. For example, the hackers may attempt to use the system to access a second system or the malware may not activate until a verification code is entered. One prime example of this was that of the Stuxnet malware,[427] which was designed to stop the operation of centrifuges at the Natanz nuclear facility, Iran. The malware was first installed on the SCADA systems of the facility and tests were run to ascertain that these systems were connected to the target centrifuges.[428] Until such tests were executed and the connection was verified, it is inaccurate to claim that the SCADA system itself or the centrifuge were the targets of the act of violence.

On the whole, rationalising via forming an analogy between a physical space and a cyberspace is fraught with problems; they represent extremely different environments in which behaviours and actions are very divergent. From a legal perspective, it is more productive to delineate the elements that represent an attack, including the means, method, and target, and then, where necessary, define a relevant analogy. For example, one method of using malware involves embedding it in files. In such cases, the attack occurs at the point at which the user downloads an infected file and the malware installs itself on his or her device. If the malware is installed directly onto the user's computer by a hacker circumventing the firewall, the attack occurs at the point at which the malware leaves the attacker's computer because all the fundamentals required for the legal evaluation of the attack are in place at that moment.

In the same way that mine-laying operations resulted in an extension to the API definition of attack, cyber-attacks now also need to be taken into consideration. The destructive potential of a mine is intrinsically limited to the region immediately surrounding the device. As such, a person who is at risk of harm from the mine due to being within the destructive reach of this mine becomes the potential target. Malware can pass through many different systems and networks before it reaches

[427] Jackson Maogoto, *Technology and the Law on the Use of Force* (Routledge, 2015) 53.
[428] Thomas Chen and Saeed Abu-Nimeh, 'Lessons from Stuxnet' (2011) 44(4) *Computer* 91.

the premeditated target, and a user of these systems and networks may take action that facilitates the progression of the malware until it reaches the end target. While this does not change the standard related to the identification of an attack or the proposed target, it does introduce an element of complexity into the process by which all the actors who are involved in an attack are identified.

Cyber Hacking, Ruses and Human Accountability

Future conflict may be shaped by stealthy and widespread cyber hacking, designed either to deny or corrupt datasets central to an opponent's targeting decisions. If this is the case, there may be legal implications for the use of remotely operated and autonomous weapon systems for the purposes of launching military attacks. Existing law on this matter centres on the narrowly-defined concepts of enemy wounding and capture,[429] treacherous killing and perfidy, along with the abuse of protected symbols.[430] Provided these rules are obeyed, existing law does not prohibit cyber activities that are designed to corrupt an enemy's battlespace picture or to degrade their infrastructure, preventing them from effectively launching attacks or abiding by distinction, proportionality and precautions rules.

Indeed, it is likely that such cyber hacking will involve the use of autonomous weapon systems, piloted from a remote location. Arguably, the legal obligations to take 'constant care' and to do 'everything feasible' would imply that all possible efforts would need to be made to ensure that any unmanned operations employ sufficiently robust systems. This would mean that once it became possible for datalinks, guidance systems, weapon control systems and targeting software to be digitally compromised, these systems would need to be very carefully protected against any hacking activity that could render them indiscriminate. Sound military grounding for such investments would include the requirement to ensure that the correct targets are engaged. Further, these endeavours would serve a humanitarian purpose in that they would prevent any interference that could negatively affect the weapon's control and thus compromise the security of civilians and civilian objects. Potentially, by reducing or removing the links between weapon platforms and controllers and, instead, making the systems partly or entirely autonomous, the risk of cyber

[429] API, Article 37(1) and Hague Regulations 1907, Article 23(b).
[430] API, Articles 38 and 39 and Hague Regulations 1907, Article 23(f).

interference could be reduced and, in turn, better protect civilians and civilian objects from its consequences.[431]

Accordingly, although not a legal requirement, it could be advantageous for autonomous and remotely controlled weapon systems to identify cyber interference or performance issues and share this information with their operators or mission controllers. It would also be useful for such a system to automatically abort its mission if the proper performance of its targeting software were compromised by cyber interference. It is possible, however, that cyber hostilities could be so sophisticated that their intrusion or interference could be concealed. It is likely that complex legal issues will arise if, for example, a commander's operational understanding is distorted and, despite their efforts to comply with distinction, proportionality and precautionary rules, this distortion causes unintentional attacks upon civilians or civilian objects.

To assess the implications of these matters, it is important to consider scenarios in which a hacker could transmit false target coordinates, corrupt targeting data stored within a system or distort datalinks between sensors and system operators or, in the case of autonomous weapon systems, their control mechanisms. In every case, false data could mislead an autonomous system or its 'on the loop' operator, causing them to launch an attack on a civilian object whilst believing it to be a legitimate military objective.

Potentially, there could be evidence that links the attack in question to the state that operates the compromised weapon system. Furthermore, adequate detection of cyber interference could take time to achieve, if he intrusion were indeed possible to detect. Nonetheless, if such detection were to become feasible, it could be argued that in order to meet the 'all feasible precautions' obligation in Article 57, states would need to acquire and operate appropriate detection systems, especially if such interferences became likely. Future missions may well require the detection and counteraction of such interferences to ensure compliance with targeting law and achievement of their intended military purpose.

[431] Jeffrey Thurnher, 'Feasible Precautions in Attack and Autonomous Weapons' in Wolff Heintschel von Heinegg, Tassilo Singer (eds), *Dehumanization of Warfare* (Springer, Cham, 2018) 106.

Nevertheless, it is important to remember that any cyber activity designed to degrade an enemy's targeting system represents a lawful operation against a military objective. Whilst deception activity of this type will cloud an adversary's battlespace picture, it does not suggest any legal protection for them and, as such, do not constitute perfidy. Instead, such activity is intended to reduce an enemy's confidence about the precise locations of their military objectives[432] and is a classic example of lawful deception.[433] Considering cyber ruses in this way, current law only prohibits them if their sole intent is to deceive a military adversary into attacking legally protected persons or objects, civilians or civilian objects and if they are a direct cause for such results. If cyber ruses simply seek to reduce an adversary's confidence in their own targeting processes or to damage those processes, thus limiting the accuracy and reliability of attacks, they are not currently prohibited.

As such, remotely controlled and autonomous weapon systems should be designed with the following priorities in mind:

a. robust protection against hostile interference or intrusion;
b. able detection and operator or mission commander-notification of cyber intrusion or interference;
c. operator or mission commander-notification of any cyber interference or intrusion that targets the system's control mechanisms, the accuracy of the operational picture upon which its attack decisions are made, or the appropriate performance of its automated or autonomous functions;
d. operator or mission-commander notification of the effects of any cyber interference or intrusion in terms of the affected system's reliability.

Further, system design should ensure such platforms meet at least one of the following criteria:
a. mission commanders remain able to terminate missions where necessary;
b. mission commanders remain able to re-task and/or redirect the platform during the mission;

[432] The notion of perfidy under API, Article 37(1) requires, inter alia, the deception of the enemy as to protected status under the law of armed conflict.
[433] Lawful ruses of war are defined in API, Article 37(2).

c. mission commanders remain able to alter the platform's operation so that any subsequent actions are controlled by its operator;
d. the system is configured in such a way that it will take such precautions independently;
e. the system has an adequate combination of these listed abilities.

When cyber interference or intrusion allows its instigator to take control of an autonomous, automated or remotely controlled weapon system or any of its munitions, the instigator of these operations will be legally responsible for any unlawful use that follows. If such individuals are state organs or operating on behalf of a state that understands the circumstances surrounding their activity, this legal responsibility will then be transferred to the state actor.[434] Consequently, it will be vital for the weapon system operator or autonomous mission commander to understand and be able to evidence any such losses of control.

When a cyber hacker takes control of a weapon system or its munitions, they assume legal responsibility for any subsequent operation of that system or its munitions. As such, the hacker is responsible for ensuring that any such use against their opponent is compliant with the rules of distinction, proportionality and that they take the requisite precautions when launching these attacks. If the hacker interferes with their adversary's operation of the system and its weapons but does not assume control of the system, they cannot be attached to the system as an attacker, but remain bound by the obligations of Article 58 of API.

Should a hacker only take sufficient action to prevent their adversary from attacking their original target, their 'parrying' operations would not re-classify them as an attacker.[435] In such circumstances, if this 'parrying' causes missiles to strike upon civilians or civilian objects, it is suggested that the hacker should not be considered in breach of Article 51(2) or 52(1) of API. This is because, although Article 49 of API classifies an attack as any violent action towards an opponent, parrying of this nature only redirects the violent actions of another away from their

[434] ILC, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, 2001, Article 17.
[435] William Boothby, 'Highly Automated and Autonomous Technologies' in William Boothby (eds), *New Technologies and the Law in War and Peace* (Cambridge University Press, 2018) 157.

intended target; it does not see a hacker positively redirect this violence to an object or person of their choosing.

These intricacies depend upon the hacker's intent, which, in many cases, will be difficult to determine.

Should a cyber hacker compromise, for example, the precision guidance of an RPA[436] and, as a result, render it so unreliable that it could foreseeably launch indiscriminate attacks upon civilians, civilian objects or military objectives, it would be difficult to reconcile this hacking activity with the obligation to 'take constant care'.[437] In order for a hacker to be considered an attacker in this scenario, they would need to assume responsibility for initiating the operation in its eventual form and for this operation to constitute an act of violence against their opponent.

As a result of the preceding discussion, the following suggestions are made:

(1) Should a cyber hacker obtain sufficient control of an autonomous or remotely controlled weapon system to consciously or deliberately direct its munitions at, or cause the system to direct these munitions at, an objective of their choosing, they should be held accountable for the consequences of the weapon's operation.

(2) This paragraph is applicable if: (a) the level of control referred to in the previous paragraph is not achieved but the hacker still has an adverse effect on the weapon system's target recognition software or the reliability of the munition's guidance or firing systems; b) the hacker correctly expects that their actions will cause the weapon to attack protected objects or persons, civilian objects or civilians, or to perform indiscriminate attacks; and (c) the hacker causes the weapon to redirect towards specific objects or persons, as specified by them. Should this paragraph apply, the hacker should be held accountable for any consequences resulting from the weapon's use.

[436] Remotely piloted aircraft.
[437] William Boothby, 'Highly Automated and Autonomous Technologies' in William Boothby (eds), *New Technologies and the Law in War and Peace* (Cambridge University Press, 2018) 157.

(3) Should a cyber operation, in the circumstances outlined in the previous paragraph, foreseeably cause a hacker's adversary to launch indiscriminate attacks, this operation should be seen to defy the obligations of Article 57(1) and Article 58(c) of API.

(4) Should a hacker interfere with a system's guidance mechanisms for the specific purpose of deflecting its weapon away from the original target, they should not be held accountable for any damage or injury caused by the weapon thereafter; the hacker does not assume directional control of the munitions in order to use them as a weapon themselves. Their actions do not represent an act of violence as outlined by Article 49(1) of API. In such a scenario, however, both parties should be examined in terms of their compliance with Article 58 of API.

Applying Current Law to AWS

The Evolution of Targeted Killing

During the process of targeting, the "reasonable military commander" standard will always play a crucial part. Planners and commanders will make many value judgments in determining whether a target is distinct enough, whether the attack is proportional and taking adequate precautions against error. One example is the imposition on the operator of the necessity to make a subjective choice regarding the worth of the target for battlefield gain, set against the collateral damage expected. Although artificial intelligence is developing exponentially, it is not likely that in the immediate future completely autonomous weapons systems will be produced that can coherently make such judgments, which are by their very nature subjective. The inability of autonomous weapons systems to make such decisions has been used by commentators and critics to label such systems illegal.[438] This criticism is unfounded, as ultimately the autonomous targeting of such weapons will be under human control, and they have the capability to ensure that the system operates within the law.

[438] Jonathan Herbach, 'Into the Caves of Steel: Precaution, Cognition and Robotic Weapon Systems Under the Law of Armed Conflict' (2012) *Amsterdam Law Forum* 4(3) 3, 20; Markus Wagner, 'Taking Humans Out of the Loop: Implications for International Humanitarian Law' (2012) 21 *Journal of Law and Information Science* 1, 11; Markus Wagner, 'Autonomy in the Battlespace: Independently Operating Weapon Systems and the Law of Armed Conflict' in Dan Saxon (eds), *International Humanitarian Law and the Changing Technology of War* (Martinus Nijhoff, 2013) 122.

Countries will, however, be responsible for ensuring that their targeting protocols take full account of the differences autonomy brings, particularly regarding the place of subjective decisions in the process. Autonomy will mean that such subjective decisions are taken at different times to when they are made at present. Humans will continue to make the judgments, but such judgments will have to be made further back in the targeting process than was the case when humans had full control of weapons.[439] With a human operating system, decisions regarding the legality of a strike could often be made right up to the final seconds; with autonomous weapons systems, the planners must make the judgments regarding targeting whilst they still have the capability of making adjustments. As an example, if an autonomous weapon system is being sent into areas where it is likely to be unable to receive new instructions (for example into the deep ocean, or into an area where the enemy jams communications), subjective decisions must be taken before launching. Notwithstanding such divergences from traditional targeting protocols, however, if it is managed with care, then autonomous targeting can remain within the law.[440] We are going to explain this in the potential solutions section.

In order to be legally compliant, planners and programmers will have to interpose their subjective assessments at various stages during targeting. To begin with, a human operator will have to exercise close control over the preparation of the autonomous weapon. The system will receive detailed instructions from the operator, who will set target assignments, attack circumstances and collateral thresholds. Essentially, the operator envisions the subjective questions the system will be asked during a mission and sets the parameters for its answers. The autonomous system will not be autonomous in terms of making subjective judgments; rather these judgments will have been made by the operator so that the system will make solely objective decisions regarding legal engagement. For example, if the system determines that collateral damage will be higher than the parameters entered by the programmer, it will either abort its attack or refer to a human controller for further instruction.[441]

---

[439] Bill Boothby, 'Autonomous Attack—Opportunity or Spectre?' in Terry Gill, Robin Geiss, Robert Heinsch, Tim McCormack, Christophe Paulussen, Jessica Dorsey (eds), *Yearbook of International Humanitarian Law*, vol 16. (T.M.C. Asser Press, 2015) 73.

[440] Jeffrey Thurnher, 'Means and Methods of the Future: Autonomous Systems' in Paul Ducheine, Michael Schmitt, Frans Osinga (eds), *Targeting: The Challenges of Modern Warfare* (T.M.C. Asser Press, 2016) 193.

[441] Jeffrey Thurnher, 'Means and Methods of the Future: Autonomous Systems' in Paul Ducheine, Michael Schmitt, Frans Osinga (eds), *Targeting: The Challenges of Modern Warfare* (T.M.C. Asser Press, 2016) 193.

Deploying an autonomous weapon system is itself a subjective judgment requiring human input. Planners or commanders must make a subjective judgment as to the appropriateness and legality of an autonomous system for each mission. Thus, they must be fully cognizant of what an autonomous weapon system can do and have a complete understanding of the values, criteria and parameters embedded in the system. An operator must completely comprehend the ways in which the autonomous system is likely to behave in any given circumstances, and so be able to assess whether it will remain legally compliant in its actions. The operator can then make the subjective judgment as to the suitability of the autonomous weapon for the mission in question.[442]

Such subjective decisions are taken by humans prior to the attack itself, frequently further back in the targeting process them has traditionally been the case. A significant number of commentators have criticized this, with some suggesting that a time limit should be placed on military attacks so that only those where a human approves lethal force just before impact would be legal. However, the *lex lata* contains no such imposition [443], and a law of that nature could be extremely damaging. In certain circumstances, for example in the case of a cyber-attack, or reacting to a missile attack on a warship, the time for decision making may be split seconds. Delaying the process of defence or retaliation by seeking a human decision may be impractical or even life-threatening.[444]

Without an arbitrary time limit between launch and impact being set, the subjective decisions taken by human operators will have to meet a standard of reasonableness. The timing of the process will be crucial to this. The bigger the gap between the final input from a human operator and the impact on the ground, the more chance there is that there may be changes in the target area with unintended consequences. The greater the risk of this happening, the less reasonable it becomes to use an autonomous system. By building the opportunity for autonomous systems to be re-targeted by human beings into the cycle, states can reduce the risk of this happening, although such controls

[442] Jeffrey Thurnher, 'Examining Autonomous Weapon Systems from a Law of Armed Conflict Perspective' in Hitoshi Nasu, Robert McLaughlin (eds), *New Technologies and the Law of Armed Conflict* (T.M.C. Asser Press, 2014) 223.
[443] Mary E. O'Connell, 'Banning Autonomous Killing' in Matthew Evangelista & Henry Shue (eds), *The American Way of Bombing: How Legal and Ethical Norms Change* (Cornell University Press, 2013) 12.
[444] Jeffrey Thurnher, 'Examining Autonomous Weapon Systems from a Law of Armed Conflict Perspective' in Hitoshi Nasu, Robert McLaughlin (eds), *New Technologies and the Law of Armed Conflict* (T.M.C. Asser Press, 2014) 223.

may not be possible in certain circumstances, for example when working underwater or where the enemy is jamming communications. All of these risk factors will have to be taken into account if human controllers are to be judged as having been reasonable when they deploy an autonomous weapon.

There is obviously a major role for subjective judgments regarding targeting. Although fully autonomous weapon systems cannot make such judgments, they are still legal for battlefield use provided that humans have made appropriate qualitative decisions regarding targeting throughout the process of deployment. Those states intending to develop and deploy autonomous weapons will have to carefully examine their protocols in order to ensure that they remain within the bounds of the law.

Identifying the Attack

The discussion presented in this section commences with an evaluation of an attack that involves a single AWS identifying and firing at a single target. AWS could take any form, be it a ship-mounted CIWS firing at an incoming missile, an autonomous turret firing on an individual in the Korean DMZ,[445] an autonomous underwater vehicle firing at an enemy submarine, or some other form of AWS choosing and engaging a target. The outcomes of this evaluation are then extended to take into consideration an operation in which an autonomous weapon control system engages in separate incidents by which multiple targets are attacked.

The analysis of the applicability of the law related to the concept of attack to AWS is typically performed in relation to two somewhat distinct branches[446] that are applicable to various forms of weapons. If the use of a weapon has an instant effect, as is the case with guns and missiles, the attack takes place at the moment of last human involvement; i.e., when the weapon is discharged (for example, when the trigger to a gun is pulled, or a button is pressed to launch a missile). If the attack takes place sometime after the moment of last human involvement, as is the case with the activation of a mine, the action of the weapon is delayed. Some scholars have argued that it is possible to reconcile these two branches by considering the factor that is common to them both:

[445] See, e.g., Jean Kumagai, *A Robotic Sentry for Korea's Demilitarized Zone* (1 March 2007) IEEE Spectrum <http://spectrum.ieee.org/robotics/military-robots/a-robotic-sentry-for-koreas-demilitarizedzone>.
[446] Such as the case of weapons with an instantaneous effect and the case of delayed action weapons.

The point at which a specific target is defined.[447] The question that is of relevance to this chapter is: Can this concept be reasonably applied to AWS? Or, in light of the fact that AWS can involve both instantaneous and delayed action weapons, can a meaningful analogy be drawn between AWS and other weapon forms? Or is there a need to develop a discrete category with unique rules for weapon systems that incorporate autonomous abilities?

Boothby examined these questions in the context of sorties operated by autonomous UAVs:

'The time of the decision and of execution in the case of an autonomous mission would seem to be the time when the mission is launched, because that is the time when human input to the target recognition systems determines what the machine will attack. After all, for these purposes the time of execution of, e.g., a Tomahawk land attack cruise missile attack must be taken to be the time when the missile is launched, not the time when it impacts and detonates. Where autonomous, self-aware systems of the sort described in [JDN 2/11] are concerned, however, the position may be different. If such future systems replicate a human evaluative decision-making process, it would seem logical that the timing of that sort of attack decision must be taken to be the time when the system logic, which after all ex hypothesis replicates human decision-making processes, determines that the attack shall proceed. Similarly, the time of execution must be taken to be the time when the weapon is released by the autonomous platform.'[448]

This line of thinking preserves the distinction between two weapon classes; however, as opposed to referring to them using the distinct terms instantaneous and delayed action weapons, he describes the differences within the context of the degree of the autonomous capability:

'The distinction here, therefore, is between what can be described as simple autonomy, that is the mechanical implementation of a decision-making process pre-ordained by the personnel initiating the mission, and the more futuristic version of autonomy, or complex autonomy, namely the

[447] Terry Gill, Jelle Van Haaster & Mark Roorda, 'Some Legal and Operational Considerations Regarding Remote Warfare' in Jens David Ohlin (eds), *Research Handbook on Remote Warfare* (Eldward Elgar Publishers, 2017) 298; William Boothby, *Conflict Law: The Influence of New Weapons Technology, Human Rights and Emerging Actors* (Asser, 2014) 111.
[448] William Boothby, *Conflict Law: The Influence of New Weapons Technology, Human Rights and Emerging Actors* (Asser, 2014) 111.

mechanical implementation of an attack decision made by mechanical systems that replicate human evaluative decision-making processes.'[449]

The approach by which a distinction is based on the level of complexity of the reasoning that AWS employs is not without problems. The analysis presented in Chapter 1 highlighted how autonomy is a matter of degree as opposed to representing a capability that exists at discrete levels. Regardless, the incorporation of some degree of autonomous functionality does not entail that the weapon system progresses from being a form of military equipment to a legally acknowledged decision maker. As such, caution should be exercised when stating that a given AWS 'determines that the attack shall proceed' from a legal perspective. The autonomous capabilities that weapon systems possess can vary along a vast variety of dimensions; as such, it is both complicated and inaccurate to consistently apply a set of rules to AWS that are based on the abilities that they have at a given time.

It is important to acknowledge that the word autonomous is by no means a clear-cut description of the how a weapon system behaves and a given system's ability to operate without human intervention does not inherently mean that analogies can be drawn between these systems and other weapon forms. For example, some weapon systems have a limited degree of autonomy that makes them comparable to missiles,[450] others bear more resemblance to mines,[451] and others still are a form of cyber weapon that can act autonomously. As technologies develop, it is highly likely that AWS of the future will not be analogous to any form of existing weapon.

In the absence of an analogy that can be universally applied to all AWS for the purposes of performing a legal analysis, there is a need to identify the factors that represent an attack in an autonomous operation. Analogies restrict the scope extend or activity of how we think a particular opinion, belief, or idea about autonomous weapon systems, therefore, preventing the ability to

[449] William Boothby, *Conflict Law: The Influence of New Weapons Technology, Human Rights and Emerging Actors* (Asser, 2014) 112.

[450] See, e.g., *Advanced Medium Range Air-to-Air Missile (AMRAAM)*, Naval Air Systems Command http://www.navair.navy.mil/index.cfm?fuseaction=home.display&key=D3FAC4AB-2E9F-4150-96646AFBC83F203E; Harpy NG, Israel Aerospace Industries <http://www.iai.co.il/2013/36694-16153-en/IAI.aspx>.

[451] See, e.g., DS Hartshorn, Mk 60 (Captor) (28 November 2009) Mineman Memories <http://www.hartshorn.us/Navy/navy-mines-10.htm>.

draft of regulations. Further, potential analogies may give a false or misleading account of the nature of a distinctive attribute or aspect of autonomous weapon systems but the nature of warfare is changing rapidly and still, we need to reinterpret definition of attack in order to perceive the intended meaning of cyber-attack which creates possible outcomes for autonomous cyber-attacks. As is the case with operations that involve other forms of weapons, all the required elements need to be present for the operation to represent an attack. Specifically, an act of violence is committed against a target. As neither the existing law nor API incorporates different definitions for attacks in relation to different forms of weapons, there is a requirement to identify a point of commonality related to the operation of the different weapons. Logically, this point is the time at which all legal elements have been satisfied.

If the point at which all the legal elements have been satisfied differs between AWS and other weapon types, for example, the time of last human intervention, the difference will correlate with variances in the way in which AWS and other weapons function. The primary functional difference that is of significance in terms of an attack is that some targeting capabilities are integrated into autonomous weapon control systems. According to the law governing cyber weapons, an operation amounts to an attack at the point at which the target is selected and preparation activities commence[452]; the execution of the attack takes place when the weapon is activated by autonomous weapon control systems. It is in this moment that the criteria of an attack are fulfilled. Prior to the activation of the weapon, no act of violence has been directed at a target. The key challenge in this regard is delineating the point at which the criteria of an attack is fulfilled in terms of the last moment of human involvement in the operation because this point will differ according to the form that the targeting functions autonomous weapon control systems take.

The first hypothetical possibility involves deploying AWS with the end goal of attacking a given target. AWS will be programmed to identify that target against specific criteria. In this scenario, the target was selected by the operators of the autonomous weapon control system; it is the role of this system to locate it. The decision to attack was made at the point the autonomous weapon

[452] Michael Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013) 106. 'The term is defined in the context of international humanitarian law and in reference to the term attack used in the Geneva Conventions.' Heather Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press, 2012) 65.

control systems was activated, and the attack itself will take place if/when a target that matches the pre-programmed criteria is identified. Kongsberg's Joint Strike Missile,[453] and ISI's Harpy loitering munition[454] represent this type of AWS.

The second hypothetical possibility is deployed in the absence of a specific description of the target that is to be attacked. In this scenario, the autonomous weapon control system is required to perform processing operations that extend beyond screening a potential target against a set of criteria. An example of this is the use of AWS in some form of protective capacity. In this scenario, AWS will be tasked with detecting an incoming threat, which will have represented an unknown variable at the time the autonomous weapon control system was deployed, and assessing whether to attack it: 'Does this look or act like something I should attack?' If the answer to this question is affirmative, it is only at this point that the target is selected. Prior to that moment, no single entity was the focal point of a violent act against which it was possible to determine compliance with the principles of distinction or proportionality. If the autonomous weapon control operation concludes that the potential incoming threat does not look or act like something that should be attacked, the operation does not result in an attack.

A further factor that is of relevance is the last possible moment at which a human can intervene with the operation of AWS before an attack is launched. The discussion presented above assumes that once AWS are deployed, they do not engage in any further interaction with a human operator before the attack is launched and a target is attacked. However, a large number of AWS that are in current use and planned for the future seek human confirmation upon identification of a target and/or execution of an attack. These operations provide human operators with an opportunity to overrule the machine's target selection.[455] In AWS of this nature, the attack decision will be made at the point in time at which the human operator confirms the machine's target or fails to override

[453] *Joint Strike Missile (JSM) Brochure*, Kongsberg <https://www.kongsberg.com/~/media/KDS/Files/Products/Missiles/jsm_web_reduced.ashx>.
[454] Harpy NG, Israel Aerospace Industries <http://www.iai.co.il/2013/36694-16153-en/IAI.aspx>.
[455] See, for example, Michael Schmitt, 'Autonomous Weapon Systems and The Law of Armed Conflict: A Reply to the Critics' (2013) 4 *Harvard National Security Journal* 231; U.S. Department Of Defense Science Board Task Force Report: The Role Of Autonomy in DoD Systems 1, July 2012. In the latter report, the Defense Board points out that 'all autonomous systems are supervised by human operators at some level, and autonomous systems' software embodies the designed limits on the actions and decisions delegated to the computer. Instead of viewing autonomy as an intrinsic property of an unmanned vehicle in isolation, the design and operation of autonomous systems needs to be considered in terms of human–system collaboration.'

the target selection. If the operator does override the target selection and, subsequently, prevents the attack against the target, the operation does not represent an attack.

It is not possible to make an attack decision without first selecting a target to attack. Regardless of whether the selection of a target is performed completely by human operators, AWS are programmed to identify targets, or AWS are directly involved in the process of selection, it is the point at which the target is actually selected that the operation results in an attack. The selection of a precise target entails that AWS have an adequate description of the target such that the only steps in the process that remain are to identify the target that matches the description of the target, follow required cautionary steps, and launch the weapon.

It is important to distinguish between simple and complex forms of autonomy. Simple autonomous systems do not make targeting decisions. The personnel that initiates the mission is responsible for these decisions and the involvement of autonomous system is limited to identifying the target and launching the attack. Complex autonomous systems have been programmed to actively participate in some elements of the process by which targets are selected.[456] This activity, in combination with the decision to operate AWS at a predetermined place and time, represents the same targeting decision. It is not technically accurate to claim that the control software makes a targeting decision. To do so, would involve humanising the weapon system and recognising it as a legal decision-making entity. In the case of AWS, the targeting decisions are made by human operators who initiate the system on the understanding that it may execute an attack against a given target, though those choices do not manifest until the software runs.

In light of the above, there is no need to distinguish between different types of attacks with different weapons; regardless of the process by which the decision is made, an operation is considered to represent an attack at the point at which a target is selected and the process of activating a weapon commences. The same is true of a manually operated weapon system. The only difference between the two concerns whether one or more actions within the targeting process are performed by the software that is incorporated in the control system of the weapon.

[456] At the least, those personnel may be assumed to be aware that part of the target selection process is so encoded.

Returning to the earlier discussion of how a mine attack occurs at the point at which the target is 'immediately endangered,' it is worth noting that simply firing a weapon at a given target does not automatically lead to harm, nor does endangering a target. There is a chance that the shot will miss the target, the system that guides the missile may malfunction, or the target may defend itself. However, in the standard course of events, the target will suffer in some way, shape, or form from the attack. Firing a shot at a target endangers it in the same way that an individual in proximity to a mine is in immediate danger before it explodes.

Similarly, in situations in which cyber-weapons have the capacity to operate autonomously and select their own targets, the definition of a cyber-attack that was presented in *the Tallinn Manual* applies as customary international law.[457] According to *the Tallinn Manual,* the attack takes place at the time at which the malware is introduced to the target system. If there is a requirement for a human operator to confirm execution after the malware has selected the target, be it before or after it has reached its target, human confirmation must be provided for the operation to represent an attack. However, systems can operate without the need for such confirmation, as is the case with Stuxnet:

'Considering that there was very good chance that no Internet connectivity would be available (only access to the internal network), Stuxnet developers put all of its logic in the code without the need of any external communication. As such the Stuxnet was an autonomous goal-oriented intelligent piece of software capable of spreading, communicating, targeting and self-updating; …'[458]

If, theoretically speaking, Stuxnet was to be released during an armed conflict, there is a high chance that the form and extent of the damage it was designed to cause would entail that it legally classifies as a computer network attack.[459] In such a situation, the point of attack would be the

[457] Dan Efrony & Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' (2018) 112(4) *American Journal of International Law* 657; Eric Jensen, 'The Tallinn Manual 2.0: Highlights and Insights' (2017) 48 *Georgetown Journal of International Law* 735.
[458] Stamatis Karnouskos, 'Stuxnet Worm Impact on Industrial Cyber-Physical System Security' (Paper presented at IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society, Melbourne, Victoria, Australia, 7–10 November 2011) 4492.
[459] Michael Schmitt, 'Classification of Cyber Conflict' (2012) 17 *Journal of Conflict and Security Law* 245, 251-2.

moment at which Stuxnet entered the system that controlled the centrifuges having executed all associated steps in the target selection process including confirming the model and make of the centrifuge control system and ensuring that the centrifuges were operating at the appropriate speed to be attacked.[460] At this point in time, the only step outstanding in the process of the attack was to execute the command that resulted in the damage to the centrifuge system.

Preparatory Obligations Relate to the Combined Actions of Software and Humans

AWS control systems incorporate a number of functions that the IHL assumes are performed by human operators during the process of planning and launching an attack; for example, target selection. If these functions are taken beyond the control of humans and become controlled by the autonomous system, humans no longer perform them in the process of activating the weapon system, as the software is typically executed following the last point of human participation in the attack. However, from a legal perspective, these functions remain a fundamental part of the precautionary measures that are mandated by law. Essentially, the obligations related to preparing for an attack remain with 'those who plan or decide upon an attack'; however, in this case, the preparation for an attack is performed by executing code as opposed to human operators taking direct action. The precautionary steps that the human operators perform before activating AWS—for example, choosing the place and time of activation—in addition to those that have been encoded in autonomous weapon control systems and those that may be performed by a human operator who is responsible for monitoring AWS after they have been activated, must satisfy all the obligations related to planning and conducting an attack.

Extended Operations

According to the discussion presented above, in a situation in which AWS are deployed against an enemy and its control system selects a target and activates a weapon, the operation in its entirety represents an 'attack' for legal purposes. This is the case regardless of whether the attack targets one or more objectives. However, the legal definition of an attack is typically applied to operations that are limited in space and time, directed at a well-defined objective or set of objectives. Is there a limit as to how extensive an operation is for it to be treated as a single attack? If an autonomous

[460] Stamatis Karnouskos, 'Stuxnet Worm Impact on Industrial Cyber-Physical System Security' (Paper presented at IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society, Melbourne, Victoria, Australia, 7–10 November 2011) 4490-1.

platform is positioned in adversary territory over a prolonged period of time, during which it engages with multiple targets during numerous distinct occurrences, is there a point at which the operation should be broken up into different attacks for legal purposes? If this is the case, how is the tolerable extent of an attack determined in the context of AWS operations, and what obligations do the attackers have at the start and finish of each individual attack?

At present, the formal law[461] does not explicitly limit the extent of an attack; as such, it may appear that there is no need to demarcate the discrete attacks that are executed during a long-term operation. However, if the legal notion of an attack is to achieve its objective of limiting combatant actions, there is a need to suitably constrain the concept itself in terms of extent and form; if the concept of an attack can be extended to incorporate any indiscriminate set of actions that a combatant takes, the ability to exclude actions that would breach other rules of IHL is lost:

'there has to be some spatial, temporal, or conceptual boundaries to an attack if the law is to function. … If attacks were not conceptualised and subject to legal judgement at the tactical level, but only say the broad strategic level, then a large operation may be determined to be permissible (on the basis of broad anticipated outcomes) whilst containing multiple individual actions that would in themselves be legal violations.'[462]

It may appear that temporal or spatial limitations can be readily applied; however, there is only an incidental relation between the temporal and spatial extent of an attack and the legal implications; the temporal and spatial extent of the event cannot be applied in meaningful way to attacks that take place in cyberspace as opposed to physical space. In the case of cyberspace attacks, a conceptual limitation is required in place of temporal or spatial limitations. If the concept of an attack represents the means by which enemy actions are obliged to comply with the requirements of IHL, the conceptual limitations associated with attacks should be articulated in the context of those requirements.

[461] *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts*, art. 49.1, June 8, 1977, 1125 U.N.T.S. 3.
[462] Article 36, 'Key Elements of Meaningful Human Control' (Background paper to comments prepared by Richard Moyes, Article 36, for the CCW Meeting of Experts on AWS, April 2016) 3.

A variety of the rules contained within the IHL are designed to restrain an attacker's actions during an attack. Some of these rules can be applied to every objective attacked; for example, the requirement to ensure that the targets of an attack are military targets and not under some form of protection. Other limitations can be applied to the attack as a whole. The most basic whole-of-attack constraints that are applicable to all attacks are as follows:

• The responsibility to ensure attacks are only launched at direct military objective or objectives 'the attack on which may be expected to cause the least danger to civilian lives and to civilian objects.'[463]

• The responsibility to '[r]efrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated'.[464] This is reinforced by the supplementary requirements to precisely evaluate both the expected 'concrete and direct military advantage' and the potential harm to civilians.

• The obligation to '[t]ake all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects.'[465]

To accomplish its objective of ensuring an attacker's actions are lawful, the extent of the attack should be limited to the degree that the conduct of each component of an attack cannot diverge too significantly from comportment that would be deemed to be permissible in its own right; e.g., there could be substantial latitude for abuse if attackers were permitted to cause major harm to a civilian population in the process of pursuing a military goal on the basis that this harm would be balanced out at a later date by lesser harm in pursuit of later objectives that were treated as part of the same attack within the proportionality assessment.

[463] API art 57(3).
[464] API art 57(2)(a)(iii).
[465] API art 57(2)(a)(ii)

In addition, there is an implicit requirement for the attacker to secure sufficient intelligence in advance of an attack to ensure that the appropriate method of attack is selected and facilitate an accurate and reliable evaluation of the military advantage and civilian harm that would result from the attack.

As the constraints listed above are all directly attendant to an attacker's ability to conform with the required standard of conduct, the extent to which an attack must be limited would reasonably vary according to the circumstances in which it takes place. This includes consideration of the technology that is available to the attacker.[466]

It is reasonable to assume that this same proviso would be applicable to any form of attack preparation that is performed using technology. The outcome of such an assumption is that the attack must be confined to an activity span that adheres to the following two conditions:

1. The attacker can conduct all whole-of-attack obligations related to preparation to an acceptable standard. The factors that may limit the attacker's ability to achieve this are the technical resources that are available, the information that is available, and factors related to the distinct situation in which the attack is planned.
2. The attacker does not have the scope to cause unwarranted and disproportionate harm when attacking individual objectives that would serve to undermine the humanitarian intentions that underpin the precautionary obligations dictated by law.

If these two conditions serve to limit the scope of an attack to a span of activity that is unable to span the entire operation, there would be a requirement to conceptually apportion the operation into multiple attacks. Every one of these attacks would represent a segment of activity for which the attacker can adhere to the whole-of-attack preparatory obligations to the required standard. The attacks that form the full operation would then be demarcated by autonomous weapon control

[466] Claude Pilloud and Jean Pictet, 'Protocol I – Article 57 – Precautions in Attack' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 682 [2199]; Michael Schmitt, 'Precision Attack and International Humanitarian Law' (2005) 87 *International Review of the Red Cross* 445, 460.

systems that performs each preparatory task (selecting objectives, estimating civilian harm, and so on), taking into consideration the next planned attack.

These legal obligations place the legal responsibility for compliance on human beings as opposed to AWS. Article 57(2)(a) of API stipulates that, '[t]hose who plan or decide upon an attack' are directly responsible for such an attack. It is reasonable to assume that the individuals who were involved in formulating API would have expected individuals who have responsibilities for planning attacks to have made relevant decisions in person in advance of the execution of each attack. Various contributors to discussions on AWS have also argued that there is a distinct requirement for direct human intervention during the preparation stage of every attack. For example:

'Recognition that human legal engagement must occur over each attack means that a machine cannot proceed from one attack to another, to another, without human legal judgment being applied in each case, and without capacity for the results of that legal judgment to be acted upon in a timely manner – i.e. through some form of control system. Given that an attack is undertaken, in the law, towards a specific military objective that has been subject to human assessment in the circumstances at the time, it follows that a machine cannot set its own military objective without human authorization based on a human legal judgment.'[467]

A literal interpretation of the phrase 'decide upon an attack' that is contained within API appears to be aligned with this view. However, this literal interpretation fails to discount the chance that the process of coding software while planning an attack, and subsequently activating the software, would also represent a decision. The human intervention arguments are based on the notion that programming software via a series of decisions that are ultimately coded into that application does not represent human judgement, even in situations in which the underlying algorithm might be purposely designed to duplicate the logic a human would apply to make a decision. The process by which the military status of an attack objective is evaluated and potential civilian harm is estimated are as much an application of human engagement when it is programmed into software

[467] Article 36, 'Key Elements of Meaningful Human Control' (Background paper to comments prepared by Richard Moyes, Article 36, for the CCW Meeting of Experts on AWS, April 2016) 3.

as it is when a human operator makes a real-time decision. The extent to which humans are involved in the preparation activities that support each attack will vary according to the capabilities of the autonomous weapon control system. If an autonomous weapon control system is unable to support a precautionary task without assistance, for example, performing the complex and context-based proportionality assessment, there is a requirement for direct human intervention during the process of preparing for the attack. However, if the autonomous weapon control system has the capability to perform all the preparatory tasks to a sufficient standard that the attack that results is in full compliance with legal obligations, it is challenging to maintain the argument that the IHL regulations require the personal intervention of a human.

Other Precautions in Extended Operations

API Article 57(2)(c) dictates that '[e]ffective advance warning shall be given of attacks which may affect the civilian population, unless circumstances do not permit.' However, it does not delineate how, when, by whom or to whom such a warning needs to be issued. In the majority of cases, these factors would depend on the circumstances of the attack; however, the fundamental requirement to ensure civilians are given sufficient warning of the impending attack remains.[468]

As decisions related to whether to issue a warning will vary according to the circumstances of the attack, an autonomous weapon control system on a protracted operation that may involve multiple attacks can employ two potential approaches. It must either operate under the requirement for a human operator to issue a warning prior to commencing the attack, or have the ability to assess whether civilians will be affected by the attack and whether issuing a warning would undermine the potential for the attack to be a success and, subsequently, make a decision as to whether to issue a warning based on these evaluations.

After an attack has been initiated, it 'shall be cancelled or suspended if it becomes apparent that the objective is [protected for various reasons].'[469] This article hints at human involvement in that the party to whom such problems would 'become apparent' would typically be the human combatant who is executing the attack. It is accepted that in situations in which the selected means

[468] Ian Henderson, *The Contemporary Law of Targeting* (Martinus Nijhoff, 2009) 188.
[469] API art 57(2)(b).

of warfare does not allow the combatant to accurately perceive the target, these problems would not become apparent; as such, in these circumstances, this article 'will be likely to have little to no operation vis-à-vis the person executing the attack.'[470]

However, there is a likelihood that AWS operations will emerge in the future within which there is a significant considerable gap, in both time and prevailing events, between the time at which humans were last involved and the autonomous weapon control system executes an attack. In such situations, the probability of conditions changing in ways that were previously not anticipated will be significantly increased. Incorporating the ability for AWS to cancel or suspend planned attacks may be required to ensure that risk of causing civilian harm is appropriately managed in compliance with the underlying objectives of API.[471]

Summary

AWS operations represent an attack (an attack decision is made) at the point at which a target is selected and the preparations for using the weapon commence. Depending on the capabilities of the autonomous weapon control system and the context of the operation, a human operator or automated system may select the target and communicate this information to the autonomous weapon control system, which subsequently starts to locate the target of interest. Alternatively, the target selection may be performed by AWS themselves based on the target selection criteria. The attack is launched when an autonomous weapon control system activates a weapon that is attached to the system.

Not all AWS operations against an opponent will be concluded in one single attack. To adequately fulfil its objective to guide the conduct of combatants, the legal notion of what represents an attack must be appropriately constrained. Some precautionary responsibilities relate to the specifics of the objective to be attacked (such as confirming military status), while others are more holistic (such as determining military advantage and assessing the risk of secondary civilian harm). The whole-of-attack obligations limit the extent of what AWS can consider to represent a single attack.

[470] Ian Henderson, *The Contemporary Law of Targeting* (Martinus Nijhoff, 2009) 183.
[471] As it is in relation to attacks conducted with other weapons: Marco Sassòli, 'Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified' (2014) 90 *International Law Studies* 320.

If AWS cannot perform the required tasks within the context of the entire operation, notionally, there is a requirement to treat the operation as a series of individual attacks. In such a scenario, the whole-of-attack preparatory tasks need to be performed for each individual attack. If AWS do not possess the technical capability to perform the required activities to the standard dictated by law without some degree of human involvement, such human intervention during, or between, attacks are required.

Potential Solutions

The investigation above makes it clear that using autonomous weapons systems will raise many problematic legal issues. However, we must question whether this means that autonomous weapons systems cannot be deployed and remain within the Law of Armed Conflict until such time as computerized decision-making matches or even surpasses that of humans. As the title above indicates, we are not of this view. There are several ways that safeguards can be placed on autonomous weapons to override such problems and so dramatically lower the chances of violations of Law of Armed Conflict occurring.

It should be clear from the outset that self-targeting weapon systems are not suitable for every mission. Those in command on the battlefield must be at pains to examine if the deployment of autonomous weapons is the best solution available or if a safer or more expedient alternative exists. However, once the decision has been taken to deploy an autonomous system, commanders should adapt the mission so that it does not present the weapon system with any challenge beyond its capability. Conversely, and of equal importance, the weapon system must be modified using programming specific to the mission so that it can complete the mission without transgressing Law of Armed Conflict.[472]

Obviously, this means that planning and programming are essential parts of the process, particularly with reference to weapon systems that do not use direct real-time human operator control, as this will essentially be the last stage before the machine takes over. When there will be no human input post-launch/activation, it is vital that it is ensured beforehand that only legitimate

[472] Iben Yde, 'The Push Towards Autonomy: An Insight into the Legal Implications of Self-targeting Weapon Systems' *Royal Danish Defence College* 13.

targets will be engaged and that the machine knows not to engage targets if the damage to anything but the target will be excessive. As battlefields are highly complex environments, and distinctions regarding target identification and proportionate force require considerable analysis, it is unlikely that any present system, or any in the immediate future, will be capable of making these assessments autonomously. This means that missions must be designed in such a way that no decision regarding distinction or proportionality will be given to the machine. This can be done provided the system has built-in restrictions regarding target identity/type, attack timing, dimensions of operating zone, parameters of collateral damage, what should be done when circumstances alter, and how much direct real-time human operator can come into play.[473]

As an example, the system can be programmed to target only nonhuman, non-moving military targets that have been marked through GPS coordinates or other definite means. The machine can even be programmed with a list of targets that the operational designers have chosen. In both cases, there would be less need for the system to be able to distinguish its target.[474] To make such needs even smaller, the system could be restricted to operating in related areas with little human population, e.g. deserts or areas of ocean with little civilian traffic. Such territorial restrictions could be extremely important, particularly if the weapon system is not fixed but mobile, e.g. an unmanned aerial vehicle that is intended to roam a specific area, controlling or engaging with targets therein.

The next question that arises is that of proportionality. As previously mentioned, the legitimacy of a military target is removed if excessive collateral damage will occur through engagement. In practical terms, this is probably the most challenging element of targeting, because although a human being can assess proportionality during planning, the circumstances of an attack may swiftly change, and with them the risks of collateral damage. For example, a group of civilians might suddenly come into the target area, either accidentally or because they have been deliberately placed there as human shields; the situation has changed, and so the proportionality

[473] Iben Yde, 'The Push Towards Autonomy: An Insight into the Legal Implications of Self-targeting Weapon Systems' *Royal Danish Defence College* 13.
[474] Yoram Dinstein, 'Autonomous Weapons and International Humanitarian Law' in Wolff Heintschel von Heinegg, Robert Frau, Tassilo Singer (eds), *Dehumanization of Warfare* (Springer, Cham, 2018) 20.

of the target action must be reviewed.[475] An effective way of ensuring that autonomous weapons systems never violate the proportionality principle is to program them so that they will only engage if there is absolutely no chance of civilians being killed; however, this would dramatically undermine the usefulness of such a system for the military. An alternative modus operandi would be to assess proportionality in advance for a group of targets, and to allow the system to attack provided collateral damage levels do not exceed a specific level set by the battlefield planner or military commander prior to the operation.[476] If this means of operation was employed, a human operator might be required to monitor the entire mission with orders to modify or terminate the attack if circumstances regarding likely collateral damage change from the previous assessment.[477]

Although there are many ways that the chances of an unlawful attack occurring during programming and planning can be reduced, none of these methods are completely sufficient, as the obligation to offer protection to civilians does not end as soon as the plan is complete, nor when the weapon system is launched. The law, both treaty and customary, make it quite plain that the duty to avoid civilian casualties must be constantly observed.[478] This means that several precautions must be taken. The most vital precaution is that planners and commanders must undertake everything that can reasonably be thought of as within their power to ascertain that the target is military, and they must abort or postpone an attack if it becomes clear that either the nature of the target has been altered or that excessive collateral damage will occur; they must do this even after the mission has been launched if it is feasible.[479] With autonomous weapon systems, this means that consideration must be given as to how changes that occur in the post-planning/programming phase will be taken into consideration. One method of ensuring that this happens would be to enable the system to receive human clearance before continuing with an attack, if the system determines that the situation on the ground is significantly different to the

[475] William Boothby, 'Dehumanization: Is There a Legal Problem Under Article 36?' in Wolff Heintschel von Heinegg, Robert Frau, Tassilo Singer (eds), *Dehumanization of Warfare* (Springer, Cham, 2018) 41.
[476] Michael Schmitt, 'Autonomous Weapon Systems and The Law of Armed Conflict: A Reply to the Critics' (2013) 4 *Harvard National Security Journal* 231.
[477] Iben Yde, 'The Push Towards Autonomy: An Insight into the Legal Implications of Self-targeting Weapon Systems' *Royal Danish Defence College* 13.
[478] International Committee of the Red Cross (ICRC), *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)*, 8 June 1977, 1125 UNTS 3, available at: <http://www.refworld.org/docid/3ae6b36b4.html> [accessed 5 November 2018].
[479] Merel Ekelhof, 'Lifting the Fog of Targeting: Autonomous Weapons and Human Control Through the Lens of Military Targeting' (2018) 71 *Naval War College Review* 68.

information with which it was provided before launch.[480] This means that the system must have a data link, to allow an operator to supply it with fresh information and instructions in case s/he identifies change factors that the system has not recognized. Although there are fears regarding the ability of an enemy to hack into such data links, it is extremely desirable, and perhaps should be regarded as compulsory, for there always to be a means of allowing a human operator to intervene should an emergency arise.[481]

As can be seen by the above examples, there are a number of steps that can be taken to lessen the chances of an unlawful attack by curbing weapon system autonomy. The requirements of specific cases are of course circumstance dependent. However, in general, every effort should be taken to adhere to distinction and proportionality principle is and the risk of them being breached should be minimized to the utmost degree. Planners and commanders must take every possible step to ensure that this is the case, which includes switching weapons systems should a viable alternative be available. As Schmitt remarks, 'as a matter of law, more may not be asked of autonomous weapon systems than of human-operated systems.'[482]

Legal Use of AWS

The use of AWS inevitably means that some of the tasks involved in the targeting process are no longer directly controlled by humans. The main question that is of interest in this context concerns which activities, if any at all, should remain under the control of humans in order to comply with legal requirements and what degree of knowledge are human operators required to have concerning the activities of AWS.[483]

The ultimate feature of AWS that are of interest in this dissertation is the ability to replicate a process by which a human decides to use, and subsequently deploys, a weapon. The factors that

[480] Jeffrey Thurnher, 'Feasible Precautions in Attack and Autonomous Weapons' in Wolff Heintschel von Heinegg, Robert Frau, Tassilo Singer (eds), *Dehumanization of Warfare* (Springer, Cham, 2018) 111.
[481] Iben Yde, 'The Push Towards Autonomy: An Insight into the Legal Implications of Self-targeting Weapon Systems' *Royal Danish Defence College* 13.
[482] Michael Schmitt, 'Autonomous Weapon Systems and The Law of Armed Conflict: A Reply to the Critics' (2013) 4 *Harvard National Security Journal* 231.
[483] For another study of human decision-making in AWS targeting processes see Jeffrey Thurnher, 'Examining Autonomous Weapon Systems from a Law of Armed Conflict Perspective' in Hitoshi Nasu and Robert McLaughlin (eds), *New Technologies and the Law of Armed Conflict* (Asser Press, 2014) 223.

the machine will process may include aspects related to the civilian versus military status of the potential target and the harm that may be caused, among others. It is for this reason that some observers insist on personifying AWS such that they are more comparable to combatants than weapons. However, it is not the need for AWS to engage in decision-like behaviours that throw into doubt their legal status. It is the fact that they have the ability to engage in these behaviours and subsequently launch an attack after the last point of human involvement.

The use of systems that incorporate decision support systems and ISR platforms is by no means new, and many such systems do include some level of autonomous capability. However, they do not prompt legal uncertainty to the same extent as AWS because their role is limited to the period before a human operator makes a decision as to whether to launch an attack. Their involvement is limited to producing and assimilating information on which a human decision-maker can then make a judgement that complies with the requirements of the IHL.

AWS are different on the basis that that they involve delaying an element of the human decision making until after the system is deployed. This can be some time after the last point of human involvement. As described above, the decision itself is not deferred in the sense that responsibility for this decision is passed to the autonomous weapon control system as a decision-making entity. AWS are computer-based weapons, like any other advanced weapon systems. The underlying control system is not capable of making legal decisions; it simply executes the decisions that were made at an earlier date by the human programmers and operators.[484]

However, there is a limitation to the decision that the operators of AWS, or even their commanding officers, can make when deploying these systems. The extent to which the decisions that are made are within the realms of the law given that some actions are, by the nature of the system involved, taken after the autonomous weapon control system is deployed is questionable. An individual who is responsible for planning an attack is required to '[d]o everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects';[485] however, in some cases,

[484] Jeffrey Thurnher, 'Examining Autonomous Weapon Systems from a Law of Armed Conflict Perspective' in Hitoshi Nasu and Robert McLaughlin (eds), *New Technologies and the Law of Armed Conflict* (Asser Press, 2014) 223.
[485] API art 57(2)(a)(i).

AWS are directly responsible for performing some degree of verification after human involvement. In this scenario, is it true that the planner of the attack has met the legal obligations associated with activating the autonomous weapon control system? A review of the practices that are currently in use reveals that many systems do not require the attack planner to personally perform the verification process for each of the potential targets prior to the activation of the system. For example, a number of States currently useIAI's Harpy to identify and annihilate radar-emitting devices. To achieve this, the system performs an element of the target verification process, and there has been no suggestion that this is any way illegal. However, hypothetically speaking, an autonomous weapon system could be developed that can be activated with its human operators having little-to-no knowledge of the actions it may decide to take in the process of warfare. Even if this hypothetical weapon system did ensure attacks were launched within legal requirements, shouldn't there be some minimum threshold of knowledge, some minimum role within the decision-making process, that a human operator needs to legally complete before AWS can launch weapons? Or could the planning and execution phase of an entire attack be legally performed by AWS?

This chapter is not designed to represent an all-inclusive guide to the legalities of performing targeting activities with AWS. In fact, the diverse and complex nature of contemporary conflict situations entails that it would not be possible to achieve such an undertaking within the scope of this work:

'Targeting decisions and the execution of the use of force in a modern conflict can range from factually very simple to extremely complex. At one end of the spectrum, a soldier may observe a person, conclude that the person is an enemy combatant, and shoot at that person. At the other end of the spectrum, a vast amount of information from various sources may be analysed to determine that an enemy combatant will be in a certain building at a certain time. Further work is then undertaken to determine where that building is geographically located. A pilot, who never sees the information that supported the analysis, is tasked to bomb the building. The attack may be conducted using a laser-guided weapon where the laser designation is provided by yet another person.… '[486]

[486] Ian Henderson, *The Contemporary Law of Targeting* (Martinus Nijhoff, 2009) 233.

Rather, the intention of the discussion presented thus far is to provide an overview of just some of the complications associated with the legalities of the role of AWS in planning and launching attacks and the current limitations that the law of targeting inflicts on the application of AWS. The framework employed here is that of the IHL six-step targeting process that was presented by Henderson; [487] however, the discussion has wider application within alternative targeting processes.[488]

Without intending to participate in the ongoing debate surrounding the ways in which AWS may be utilised by the armed forces in the future, it is apparent that the legal ramifications of the application of autonomous systems will be greater in the case of dynamic targeting situations than in premeditated strategic attacks that utilise specific targeting. In situations in which the plan that underpins an attack is developed far in advance of the attack itself through the involvement of the appropriate personnel, there is less likelihood that AWS will independently engage in target selection and verification. In such cases, the responsibility of AWS would be limited to precisely engaging the clearly delineated target using the pre-approved method of attack. The ability of the weapon system to determine the legal implications of attacking a given target in the absence of human intervention would be of more significance in situations in which dynamic targeting is employed or previously unanticipated targets arise.

The legal obligations set out in Article 57(2)(a) of API in relation to the planning stage of an attack are covered by the first four phases of the IHL targeting process. During this phase, the legal burden rests on 'those who plan or decide upon an attack'.[489] The nature of this burden would not vary whether it was a human or automated weapon control system that executed this stage of the attack. In the same way that the weapons law obligations explained in Chapter 2 did not change as a result of additional functions being added to the weapon's control system, the legal obligation related to making targeting decisions also does not change.

[487] Ian Henderson, *The Contemporary Law of Targeting* (Martinus Nijhoff, 2009) 234.
[488] See, e.g., Mark Roorda, 'NATO's Targeting Process: Ensuring Human Control Over and Lawful Use of Autonomous' Weapons' (2015) 6 *Amsterdam Center for International Law*.
[489] For a general discussion of the importance of precautionary obligations to use of AWS see Jonathan Herbach, 'Into the Caves of Steel: Precaution, Cognition and Robotic Weapon Systems Under the International Law of Armed Conflict' (2012) 4(3) *Amsterdam Law Forum* 3.

The first two steps of the IHL targeting process relate to Article 57(2)(a)(i). This mandates that attack planners must:

'Do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives … and that it is not prohibited by the provisions of this Protocol to attack them.'

The first activity that Article 57(2)(a)(i) requires, to identify and observe the target and the area in which it is located, does not particularly represent a major issue with regards to AWS. This stage in the process involves gathering intelligence. The use of some form of autonomous system as opposed to manual means for ISR activities would only introduce legal questions if that system could autonomously decide to manipulate the raw data that its sensors acquire in such a way that it actively influenced the outcome of any decisions that were made based on that data.

The second activity involves applying the legal tests that are outlined in API to the information that has been collated to facilitate a decision related to the legal status of the proposed target; for example, does it represent a military objective? Is this military target subject to special protection? While these questions ultimately result in some form of legal judgement, they do not necessarily need to be probed by a lawyer[490] or even, perhaps, by a human being. Essentially, this step involves drawing a comparison between the information that has been observed about the target and the position in which it is located and the criteria that represents military objectives. There appears to be no legal barrier that prevents this analysis from being performed by a software system as opposed to a human being; however, it is likely that several practical challenges will emerge in relation to ensuring that all the required information from a vast array of sources is available in a form that automated weapon control systems can process.

Efforts to resolve this with the rest of the planning stage are enlightening. Article 57(2)(a)(ii) relates to the third step in the process:

[490] Jonathan Herbach, 'Into the Caves of Steel: Precaution, Cognition and Robotic Weapon Systems Under the International Law of Armed Conflict' (2012) 4(3) *Amsterdam Law Forum* 234.

'Take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects.'

While Article 57(2)(a)(iii) relates to the fourth step:

'Refrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.'

At face value, a logical inconsistency is apparent: AWS must be selected as the means of attack before any questions related to how it is used to identify targets or execute proportionality assessments arise. However, according to the written law, the means of attack must be selected based on the information that was gathered in the previous steps. At a minimum, the commander needs to be confident that a given AWS is capable of successfully attacking the selected target before it is indicated as a means of attack.

This highlights one limitation, albeit a soft limitation, on the decisions that can be realistically delegated to AWS. To select AWS for use in an attack, the commander must know that AWS can:

• Identify the chosen objective within its environment and, correspondingly, have the capability to abstain from incorrectly selecting other people or objects as objectives;

• successfully attack the desired objective with the weapons it has at its disposal;

• represent the means by which the chosen objective can be attacked while causing the least potential harm to civilians.

To achieve these goals, AWS will need to acquire some knowledge of the target and their surroundings in advance of the attack.[491]

For example, after launch, the IAI Harpy can operate completely without any human intervention. No input is required to help the Harpy detect enemy radar installations, either by directing it to such installations or confirming the target selection in advance of the attack. The decision to activate the IAI Harpy must be based on an earlier human decision making processes that ascertained that the destruction of enemy radar installations is a militarily requirement, the activity of civilians or protected subjects within the area in which the installations are believed to be installed is not such that using the Harpy would be insufficiently discriminate, and that the explosive device activated by the Harpy can destroy the type of radar installations that the enemy is believed to be operating without causing any excessive damage or harm beyond that objective. The attack decisions that are involved with other AWS should be based on similar analysis.[492]

Once the planning process has been conducted in full, the attack will progress into the execution phase. Step five of the IHL targeting process relates to initiating and executing the attack and the associated legal requirement is outlined in API art 57(1):

'In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects.'

When a weapon system that is manually operated is deployed in an attack, the legal responsibility for the processes involved in this phase lie with the combatants who are directly operating the weapon system involved; for example, the pilot of an aircraft that fires missiles. If the use of an autonomous system serves to reduce or eliminate the involvement of the combatant, no other person may be in a suitable position from which to assume 'constant care' for the conduct of the attack. However, the weapons law rule that is outlined in API Article 51(4) prohibits indiscriminate

[491] Robert McLaughlin, 'Unmanned Naval Vehicles at Sea: USVs, UUVs, and the Adequacy of the Law' (2011) 21(2) *Journal of Law, Information and Science* 100, 105.
[492] Jeffrey Thurnher, 'Examining Autonomous Weapon Systems from a Law of Armed Conflict Perspective' in Hitoshi Nasu and Robert McLaughlin (eds), *New Technologies and the Law of Armed Conflict* (Asser Press, 2014) 222.

attacks. Specifically, the rule in Article 51(4)(b) that outlaws' attacks 'which employ a method or means of combat which cannot be directed at a specific military objective' would necessitate that AWS control software does not direct an attack at a civilian target. Further, Article 57(2)(a)(iii) contains an injunction that requires combatants to avoid making a decision to launch any form of attack that can potentially cause excessive civilian harm. This implies that AWS must possess the capability to avoid causing civilian harm and, as such, the operators would need to develop an in-depth understanding of how a given autonomous weapon system will potentially behave in the context of the attack.[493] In combination, these two stipulations appear to have a considerably similar effect on AWS that Article 57(1) would have on a human combatant launching an attack. Finally, step 6 of the IHL targeting process relates to API Article 57(2)(b). This necessitates that an attack is abandoned or deferred if there is a change in circumstances or new data becomes available. The basic duty to suspend or cancel the attack in such conditions 'is imposed upon anyone who has effective control over the attack. This might be the person conducting the attack or it might be a commander who can issue orders to the person conducting the attack.'[494]

However, there does not seem to be an unequivocal requirement for a combatant to maintain the ability to cancel or postpone an attack after it has been initiated, though there is undoubtedly an assumption that these options will be possible until a point close in time to when harm is caused to a target:

'It is principally by visual means - in particular, by means of aerial observation - that an attacker will find out that an intended objective is not a military objective, or that it is an object entitled to special protection. Thus, to take a simple example, an airman who has received the order to

[493] Jeffrey Thurnher, 'Examining Autonomous Weapon Systems from a Law of Armed Conflict Perspective' in Hitoshi Nasu and Robert McLaughlin (eds), *New Technologies and the Law of Armed Conflict* (Asser Press, 2014) 224.

[494]Jeffrey Thurnher, 'Examining Autonomous Weapon Systems from a Law of Armed Conflict Perspective' in Hitoshi Nasu and Robert McLaughlin (eds), *New Technologies and the Law of Armed Conflict* (Asser Press, 2014) 237; Claude Pilloud and Jean Pictet, 'Protocol I – Article 57 – Precautions in Attack' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 686 [2220].

machine-gun troops travelling along a road, and who finds only children going to school, must abstain from attack.'[495]

Nonetheless, the likelihood that the ability of a combatant to cancel or suspend an attack may be reduced is deliberated:

'However, with the increased range of weapons, particularly in military operations on land, it may happen that the attacker has no direct view of the objective, either because it is very far away, or because the attack takes place at night. In this case, even greater caution is required.'[496]

It is reasonable to assume that the requirement for 'greater caution' would be more pertinent in the case of AWS that are deployed in situations in which a long period of time may pass and/or intervening events may occur between the activation of the platform and the engagement of the target. The caution exercised in this regard would involve ensuring that AWS that are selected for the attack are appropriate in these circumstances and that they are activated at the right time and place. However, that does not entail that there would be no means of terminating an autonomous attack; incorporating the functionality to do so would be the responsibility of the weapon system designers and should be based on a thorough evaluation of the humanitarian and military advantages of incorporating such functionality and maintaining an adequate level of control over the weapon system after its deployment.

The use of autonomous weapon systems (AWS) can create a greater delay between a weapon being activated and its target being struck. When an extended delay is introduced, weapons benefit from great loiter times. Military advantage can in some cases increase during the loiter period of an activated weapon. An unarmed vehicle-launched bridge, for example, offers no significant military advantage as a target. However, should this bridging vehicle then be employed by large numbers of opposition troops, its military advantage will increase over time.

---

[495] Claude Pilloud and Jean Pictet, 'Protocol I – Article 57 – Precautions in Attack' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 686 [2221].

[496] Claude Pilloud and Jean Pictet, 'Protocol I – Article 57 – Precautions in Attack' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 686 [2221].

According to Sassóli, this area of international humanitarian law represents the main argument against weapon systems that remain fully autonomous over an extended period.[497] Without being continually updated at a strategic and operational level, Sassóli holds that autonomous weapons would not be able to operate proportionally.[498] The arguments presented by Sassóli are worth considering further.

Using fully autonomous weaponry for extended time periods, it is likely that such systems will require a datalink capable of updating them on their targets' shifting military advantage. These updates, however, do not need to be constant. In the case of many targets, the military advantage will remain relatively stable, even when contrasted with the ever-evolving war picture. An opposition headquarters, for example, is likely to hold a very stable level of advantage throughout a conflict. Most likely, an AWS could be launched against such a target without any question of proportionality. In a dynamic battlespace, however, the intricacies of proportionality increase.

In a hypothetical battlespace, consider three opposition tank battalions. Each of these battalions contains fifty-eight vehicles. In order to engage these battalions as targets, the campaign commander will first develop an operational structure within which they can outline their plan of action in terms of time, space, objectives and resources.[499] They may choose to select primary and secondary objectives. In the hypothetical battlespace presented, the primary objective would be to destroy the first battalion. The secondary objective would be to destroy the second and third battalions in support of the primary efforts. Tanks in the second and third battalions thus present a lesser military advantage than those in the first battalion. Each battalion would be fired upon using a separate AWS. Each of the three AWS would be pre-programmed with the military value of the tanks within its target battalion. In this scenario, it is assumed that all individual tanks are equivalent, and that their different military advantages hinge entirely on the commander's target assessment.

[497] Marco Sassóli, 'Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified' (2014) 90 *International Law Studies Series US Naval War College* 330.
[498] Marco Sassóli, 'Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified' (2014) 90 *International Law Studies Series US Naval War College* 332.
[499] Army Doctrine Publication (ADP) 3-0, Unified Land Operations (2011).

As individual tanks were destroyed during battle, the military advantage of each remaining tank would subsequently increase. The key question in this scenario is thus how each AWS could re-evaluate the value of its remaining targets, based on the number of remaining tanks within the other battalions. Once again, it is important to consider the AWS' control functions.

Sophisticated Systems: In this scenario, an AWS would identify, and respond to, shifts in the military advantage of each target. As such, the three AWS would share a datalink, or be able to detect attrition in the battlespace and then recalculate the military advantage of remaining targets.

Operational Limitations: The first AWS could be employed for a limited time-period, or with a specific, controlled objective (e.g., destroy five targets). Operated in this manner, the military advantage of an AWS' target set would be unlikely to change significantly.

Update Rates: Human operators would update the first AWS on the status of targets within the second and third battalions.

Human Oversight: Whilst an AWS was deployed, humans would exercise control or supervision over its operating system.

Without doubt, proportionality presents a challenge for the use of fully autonomous weapon systems within the bounds of legal warfare. This challenge is particularly prevalent in a dynamic battlespace and when AWS are deployed for long periods in which the military advantage of each target is likely to change. In such a situation, legal operation of AWS would depend upon the systems' ability to account for shifts in military advantage. By applying the control methods above, operators of AWS would be able to ensure that such weapon systems were operated in accordance with the law.[500]

In terms of civilian protection, the effectiveness of an AWS versus human targeteers would depend on the command level at which the battle damage assessment is conducted. If AWS would only be

[500] Christopher Ford, 'Autonomous Weapons and International Law' (2017) 69 *The South Carolina Law Review* 413.

able to conduct battle damage assessment based on the military advantage and estimated collateral damage of their own target set and attack profile, they would only be able to calculate proportionality at the tactical level. There is, however, an international appetite for battle damage assessment to be conducted at the strategic and operational levels, considering the military advantage of an entire campaign, rather than a single strike. This study supports this view. It is important to consider AWS as one part of a larger military platform, and as a system that must recalculate its tactical battle damage assessment in accordance with proportionality assessments conducted at the strategic and operational levels.

In order to facilitate such AWS operations, the systems would need to be continually updated on developments at each level of the campaign. The AWS would then, most likely, reconduct tactical battle damage assessment in accordance with the changing battlespace. Naturally, such systems would require significant protection to prevent them from being compromised by hostile forces. However, the risk of such virtual attacks is one of the key motivations behind the development of AWS.[501]

It is feasible, or certainly will become feasible, for AWS to communicate with strategic and operational headquarters elements via datalink, and for them to, in turn, keep the systems updated on campaign developments at each level. With such information channels open, proportionality calculations would become feasible at all levels. Similarly, this would allow for real-time information to be fed back from the AWS, and operational planning to be influenced accordingly. If one AWS launched an attack and achieved the military advantage sought by a larger campaign, the military advantage of remaining targets would drop. Should AWS conduct battle damage assessment at a tactical level, disproportionate decision making at operational level would become less likely. In such circumstances, the risk of collateral damage would reduce, and protections afforded to civilians would increase.

As an alternative scenario, consider a swarm of armed drones, all operating autonomously in an urban area and tracking moving military targets. If these drones were capable of effective target

[501] Chantal Grut, 'The Challenge of Autonomous Lethal Robotics to International Humanitarian Law' (2013) 5 *Journal of Conflict & Security Law* 11.

acquisition, each of their attacks could be assumed to be proportionate. Civilian damage, could, however, be excessive, as a string of separate attacks could cut off all civilian escape routes. Should a number of AWS be deployed together, such as is the case when autonomous drones are set to swarm, battle damage assessment should be conducted on the AWS' collective effect as well as their individual effects. Further, the proportionality of such a mission should also be assessed at operational level. In this instance, calculations should combine both battle damage assessment at the tactical level and any other influence upon military advantage observed from the operational standpoint. This study holds that AWS should not conduct operational or strategic battle damage assessment without the oversight of a military commander as, beyond the tactical level, external influences come into effect when assessing military advantage.[502]

AWS could, however, use artificial intelligence (AI) for future battle damage assessment. Subject to sufficient technological advances, AI could hone battle damage assessment by uploading banks of sample calculations to AWS operating systems. It is even possible that, through a self-learning ability and consultation of a battle damage assessment reference database, future AWS could provide human operators with clearer boundaries between proportionate and disproportionate collateral damage.[503]

Conclusion

There is no doubt that enhancing the autonomous capabilities of weapon systems will have any significant repercussions in terms of targeting; however, the ability to remain in compliance with legal obligations should not be majorly impacted.

The mainstay of the required change concerns the quantity and form of knowledge that individuals who are responsible for planning an attack will need to have to ensure they comply with the law. In essence, AWS are designed to perform tasks that would otherwise be performed by humans; as such, AWS need to have access to the data that is required to perform those tasks. However, the

[502] Jeroen van den Boogaard, 'Proportionality and Autonomous Weapons Systems' (2016) 7 *Journal of International Humanitarian Legal Studies* 17.
[503] Alan Backstrom and Ian Henderson, 'New Capabilities in Warfare: An Overview of Contemporary Technological Developments and the Associated Legal and Engineering Issues in Article 36 Weapons Reviews' (2012) 94 *International Review of the Red Cross* 490.

attack planners who are contemplating deploying AWS in an assault still need to have access to in-depth information about the proposed attack and this data should be employed to inform the decision as to what, if any, AWS are used. As API Article 57 leaves the legal responsibility for decisions firmly with attack planners and executers, these individuals must have access to sufficient information to fill in the gaps associated with any precautionary decisions that AWS do not possess the capability to make autonomously. For example, it is the responsibility of humans to limit the choice of potential targets such that it can accurately identify the correct target from a range of options. In this regard, humans must either provide AWS with sufficient information or perform the proportionality assessment mandated by API Article 57(2)(a)(iii).

The extent and form of the legal requirements that impact combatants who utilise AWS, therefore, is predominantly contingent on their technical capabilities. It is not clear as to whether there is a fixed upper threshold related to the level of autonomy that can be legally granted to an autonomous weapon control system other than that human operators and planners must have the means to substantiate the decision to deploy AWS as opposed to other forms of attack.

Chapter 4 - Prohibition of Indiscriminate Weapons and Prohibition of Weapons Causing Unnecessary Suffering, Superfluous Injury

Introduction

When we examine the law regarding weapons systems, there are two relevant rule sets in IHL to consider. The first, often referred to as weapons law, is concerned with the legality or otherwise of a weapons system. This examines whether it will be legal for a state to use the system in an armed conflict. This rule set concerns the weapon system's inherent properties, what it does, and what the results will be for any humans that the property is employed against. The second rule set concerns the use of a weapons system. This details the circumstances in which the use of the weapons system can be viewed as legal. This set of rules are known as targeting law, and regulate the behaviour of those operating the weapons system, rather than the legality of the system itself.

Both of these sets of rules were created without consideration of the possibility that an autonomous system could enter into combatant operation making a significant proportion of its own decisions; therefore, applying weapons law and targeting law in this area can be confusing. Allowing a machine to act autonomously means that the human operator relinquishes certain responsibilities; those responsibilities become part of the machine's behaviour. When this happens, some actions that, in other circumstances, would be regarded as part of the way the machine was being used, instead become part of the way the machine is acting. The autonomy of the system means that it assumes parts of the targeting progress, for example, as its responsibility rather than that of a human being, so the selection of a target, assessment of collateral damage, etc. becomes a part of the machine's behaviour. Weapons law only applies to the weapon or munition; with AWS, that is only a portion of the whole system. The control system of the AWS is responsible for those aspects that may come under targeting law. It may be that, in the context of AWS, the areas of weapons law and targeting law may become conflated or need reassessment.

An alternative view of the separation of weapons law and targeting law is that the obligation to obey weapons law is generally viewed as the responsibility of the developers and the procurers of weapons systems, or those administrators who allow the systems to be used having assessed them as being compatible with international laws and treaties. Targeting law, on the other hand, is

generally held to be the responsibility of those who have planned attacks, military commanders, and those who are operating weapons. This distinction is useful when examining current laws in terms of AWS. Any behaviour of the system that is an inherent part of its operation, and cannot, or is not intended to, be changed during the course of conflict, come under weapons law and must be assessed in that light. Systemic behaviour that has been entered into the system by those who planned the attack or are operating the weapon post-deployment comes under targeting law. As an example, we may imagine a scenario in which an unmanned combat air vehicle (UCAV) that is being sent on a mission only needs to be given its target profile by human input (e.g., type of vehicle or building to attack, confines of search area, length of mission, etc.), with all decisions taken thereafter being made by the vehicle's control system. In such an instance, targeting law would come into play with reference to the human operator's decision to deploy the system in terms of what they knew about the area targeted, possible civilian presence, and the way in which the UCAV would generally be expected to act. When the UCAV is operating without human control, i.e., making autonomous decisions, that comes under the purview of weapons law. If it were to request input from a human operator, e.g., if it was having trouble identifying a target, the input the human operator had would come under the purview of targeting law.

It must be emphasised that, in law, the responsibility for selecting targets does not lie with the AWS or for those entities that designed or programmed it. Even though an AWS may contain targeting capabilities within its software, that does not make targeting selection a part of weapons law. The way in which the target is selected is simply a matter of a different process to a system that is entirely operated by humans. Military commanders and planners are still fully responsible for guaranteeing that the selected targets fall under the acceptable definitions of the relevant laws. When commanders and planners intend to using AWS, it is their responsibility to make sure that the system they have selected will use its targeting software to aim at legal targets, that it will not attack illegal targets, and that all the correct procedures will be followed to enable the AWS to carry out a legal attack. Looking at the way in which the AWS software works and ensuring that it will do nothing in terms of target selection or other behaviour that will violate IHL comes under weapons law. Testing and improving the software to ensure that this didn't happen should occur when weapons reviews are undertaken.

In terms of operations, AWS might appear to create a separation between the operator and a weapon. This is not the case, however, as military personnel in battle still have the same obligations to avoid transgressing the law; furthermore, the same obligations on those who manufacture, assess and authorise the use of AWS to remain within the law are still in place. What must be determined is not so much how AWS might change the law, but how states and their armed forces can deploy AWS without breaking extant laws.

AWS can interface with a wide range of munitions, including grenades, bombs, artillery, and nuclear warheads. These systems are capable of supporting both legal and illegal weapons. If such systems were to be accessed by non-state actors, they would very likely be used for the delivery of illegal weapons.[504] Nevertheless, this chapter will approach the matter optimistically, assuming that the weapons delivered by these systems would always be legal. This section will discuss whether these weapon systems can be considered illegal weapons *per* se, by the nature of their increased, or complete autonomy. That is, can fully autonomous, or more autonomous weapon systems inflict unnecessary suffering, or be indiscriminate, on account of their autonomy, even if the weapons they are carrying are legal? The ban on weapons that cause superfluous injury or unnecessary suffering is, of course, relevant to 'lawful means that have been altered in order to exacerbate suffering or injury'.[505] Whilst increased autonomy may not seek to increase suffering, it may render previously lawful means unlawful.

Weapon systems and their supported weapons are, as such, considered a 'complex whole', and as a set of 'related hardware units or programs or both', 'working together as parts of a mechanism', and all with a common purpose.[506] If autonomous weapons can, indeed, cause superfluous injury, unnecessary suffering or be indiscriminate, then they may contravene the fundamental principles of international weapons law. In this chapter, I examine two principal problems: first, are fully autonomous weapon systems in the strict sense weapons included under Article 36 of API to the Geneva Conventions? Second, are fully autonomous weapon systems compatible with the basic

[504] Michael Schmitt, 'Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics' (2013) *Harvard National Security Journal Features* 9.
[505] Michael Schmitt et al, *Tallinn Manual on International Law Applicable to Cyber Warfare* (2013) 144.
[506] See http://www.oxforddictionaries.com/definition/english/system (accessed 22 January 2018).

rules of weapons law (i.e. the rules prohibiting weapons that cause superfluous harm or unnecessary suffering and the rule prohibiting weapons that are indiscriminate in nature)?

Is it Possible to Define an AWS in the Strictest Sense of the Term 'Weapons' for the Purposes of Article 36 Review?

The content of Article 36 includes the terms 'weapon, means or method of warfare' but there is no definition in the Additional Protocol I,[507] therefore, an attempt to define 'weapon' or 'means and methods of warfare' is a fundamental way to understand whether a new technology characterizes as a weapon under the conditions of Article 36 legal review.

What are the 'Means of Warfare' or the 'Methods of Warfare'?

Again, there are differences in the articles of API, with Article 36 simply citing 'weapons, means or method of warfare' and Article 35 stating 'methods or means of warfare' in the first paragraph and 'weapons, projectiles and material and methods of warfare' in the second paragraph. The Diplomatic Conference Drafting Committee has been accused of ignoring its duty to guarantee consistency throughout the text.[508] Furthermore, the commentary published by the ICRC does nothing to clarify these vague terms. The only active decision made in this regard is the Committee's approval of the use of the word 'warfare' rather than 'combat' found in the draft submitted by the ICRC as warfare was considered a broader term. The ICRC later recognised that 'the term warfare encompasses combat'.[509] It is remiss of the Committee not to provide any clarification of the term methods of warfare given that this term was added to the initial description of arms, projectiles or material.

[507] The International Committee of the Red Cross' (ICRC) Commentary on Protocol I notes that 'The term means of combat or means of warfare generally refers to the weapons being used, while the expression methods of combat generally refers to the way in which such weapons are used.' [507] Jean de Preux, 'Article 36-New Weapons' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 423.

[508] William Parks, 'Conventional Weapons and Weapons Reviews' in Terry Gill et al. (eds), *Yearbook of International Humanitarian Law* (TMC Asser Press/Springer, 2005) 107.

[509]Claude Pilloud and Jean Pictet, 'Protocol I – Article 36 – New Weapons' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 398.

Typically, methods of warfare and means of warfare are synonyms because methods of warfare are 'usually understood to mean the way in which weapons are used' (i.e. the means).[510] However, the scope of this understanding is not sufficiently broad, and it is argued that methods of warfare include prohibited activities such as:

'perfidious killing, wounding or capturing of enemy combatants, denial of quarter; the murder of prisoners of war or other detained persons; attacks on civilians, as such; attacks on specifically protected objects; misuse of protective signs and destruction or seizure of property unless imperatively demanded by the necessities of war, as well as others.'[511]

The US Law of War Manual has created a draft that attempts to provide some clarity on this issue by confirming that the terms 'methods of warfare' and 'means of warfare' are not synonyms.[512] Means of warfare indicates the proposed effect of weaponry in their typical and anticipated application against the opposition. In contrast, the term methods of warfare indicate the use of weapons more generally. Historically, means of warfare has been applied in a tactical context, while methods of warfare have been employed in a strategic context.[513] Consequently, the scope of the term means of warfare includes consideration of whether an artillery shell, for instance, is legally legitimate. In other words, does the shell function as anticipated in terms of its effect on the enemy? In contrast, methods of warfare assess how the shell is used and whether its use will negatively impact innocent civilians. Correspondingly, the provision found in Article 23(a) of the Annex to the 1907 Hague Convention IV prohibiting poison and poisoned weapons is, in fact, a

[510] Isabella Daoust et al, 'New Wars, New Weapons? The Obligation of States to Assess the Legality of Means and Methods of Warfare' (2002) 84 *International Review of the Red Cross* 352.
[511] Michael Bothe et al., *New Rules for Victims of Armed Conflicts* (Martinus Nijhoff, 1982) 194.
[512] DoD Law of War Manual (draft), para. 5.003.
[513] The HPCR Manual on International Law Applicable to Air and Missile Warfare, for instance, means of warfare is understood to be 'a broader concept than weapon, for it extends also to platforms and equipment which make possible an attack.' According to that Manual, 'In aerial warfare, means of warfare include weapons, such as bombs, missiles and rockets, and the aircraft executing an attack. Means of warfare include other objects upon which the attacking aircraft directly relies to carry out the attack. For instance, aircraft which provide targeting data and other essential information to an aircraft actually engaging the target, qualify as means of warfare.' *Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare* (2010) Program on Humanitarian Policy and Conflict Research at Harvard University 41 and 55; Article 21 of the 1922/1923 Hague Rules on Air Warfare refers to 'The use of aircraft for propaganda purposes as a means of warfare' and The Swiss Criminal Code, for example, lists the use of human shields under 'Prohibited methods of warfare.' (Art. 264g) 'Targeted killings', 'rape' and sexual violence more generally in the context of an armed conflict are also sometimes described as methods of warfare. Sascha Bachmann, 'Targeted Killings: Contemporary Challenges, Risks and Opportunities' (2013) 18 *Journal of Conflict and Security Law* 30.

prohibition on a means of warfare. Traditional legal practice also bans a method of warfare as it prohibits the poisoning a water supply.[514]

Furthermore, a means of warfare can indicate a tactical approach to achieving a military goal, while a method of warfare refers to the higher-level delivery of military might. To illustrate, a method of warfare would be to starve the enemy, which can be achieved by creating a blockade or destroying crops.

The non-profit Humanitarian Policy and Conflict Research (HPRC) provides the following definition of a weapon: 'a means of warfare used in combat operations, including a gun, missile, bomb or other munitions, that is capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of, objects.'[515] This definition reveals that HPRC consider a weapon and a means of warfare as identical.

Leading commentator on weapons law Boothby agrees. Boothby asserts that weapon and means of warfare are synonymous but both are distinct from methods of warfare. According to Boothby, the means of warfare are 'all weapons, platforms [and] associated equipment used directly to deliver force during hostilities' while methods of warfare is 'the way in which weapons are used in hostilities.'[516] Therefore, a means of warfare may be a projectile, munition, implement, projectile and other type of equipment, and a method of warfare indicates how this equipment is employed in the context of a military conflict.[517] HPRC supports this view, describing methods of warfare as consisting 'of the various general categories of operations, such as bombings, as well

[514] South Africa's LOAC Manual (1996) provides: 'Objects which are essential to the survival of the civilian population (such as livestock, irrigation works and water supply) must not be attacked.' South Africa *Revised Civic Education Manual*, South African National Defence Force, 2004, Chapter 4 § 50(c). The UK Military Manual (1958) states: 'Poison and poisoned weapons … are forbidden. Water in wells, pumps, pipes, reservoirs, lakes, rivers and the like, from which the enemy may draw drinking water, must not be poisoned or contaminated. The poisoning or contamination of water is not made lawful by posting up a notice informing the enemy that the water has been thus polluted.' United Kingdom, *The Law of War on Land being Part III of the Manual of Military Law*, The War Office, HMSO, 1958, §§ 111 and 112. The US Soldier's Manual (1984) instructs soldiers: 'Using poison or poisoned weapons is against the law of war. You may not use poison or poisoning agents such as dead animals, bodies, or defecation to poison any water or food supply.' United States, *Your Conduct in Combat under the Law of War*, Publication No. FM 27-2, Headquarters Department of the Army, Washington, November 1984, p. 10.
[515] HPRC *Manual on International Law Applicable to Air and Missile Warfare* (2009) 6.
[516]William Boothby, *Weapons and the Law of Armed Conflict* (Oxford University Press, 2009) 4.
[517]William Boothby, *Weapons and the Law of Armed Conflict* (OUP, 2009) 4.

as the specific tactics used for attack, such as high altitude bombing' and the means of warfare as 'weapons and weapons systems or platforms employed for the purposes of attack.'[518]

The ICRC API commentary states that the 'term means of combat or means of warfare generally refers to the weapons being used, while the expression methods of combat generally refers to the way in which weapons are used.'[519] A similar division is drawn by the International Institute of Humanitarian Law, which states that 'means or methods is a term of art in the law of armed conflict. Means of combat are the instruments used in the course of hostilities, specifically weapons. By contrast, methods of combat are the techniques or tactics for conducting hostilities.'[520]

Looking beyond terminological considerations, the development of decision-making capabilities that are increasingly autonomous is starting to blur the lines between combatants and technology. Recent discussion of this issue by commentators in the *Journal of Philosophy and Technology* reveals how easily this distinction is confused. In this special edition of the journal, the commentators apply a variety of different perspectives. Pagallo, for one, argues that the description of a 'robot soldier'[521] is clearly beyond the scope of the categories established in international humanitarian law (IHL) and strongly implies that AWS have the potential to imitate the skills of combatants; yet other commentators examine robot soldiers uniquely as weapon types.[522] Germany's military manual also recognises that the lines between combatants and the methods and means of warfare could easily become confused, stating that 'combatants are persons who may take a direct part in hostilities, i.e., participate in the use of a weapon or a weapon-system in an indispensable function.'[523] This definition is concerned with distinguishing between different non-

[518] HPRC, *Manual on International Law Applicable to Air and Missile Warfare* (2009) 4.
[519] Claude Pilloud, and Jean Pictet, 'Protocol I – Article 36 – New Weapons' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 1957.
[520] Michael Schmitt et al, 'The Manual on the Law of Non-International Armed Conflict' (2006) *International Institute of Humanitarian Law* 12.
[521] Ugo Pagallo, 'Robots of Just War: A Legal Perspective' (2011) 24 *Philosophy and Technology* 307, 323.
[522] Linda Johannson, 'Is it Morally Right to Use Unmanned Aerial Vehicles (UAVs) in War?' (2011) 24 *Philosophy and Technology* 279, 291; Marcus Schulzke, 'Robots as Weapons in Just Wars' (2011) 24 *Philosophy and Technology* 293, 306.
[523] Military Manual of Germany, as quoted in Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law* (Cambridge University Press, 2005) 13.

combatant members of the military, yet it also accurately reveals the circularity and challenges of distinguishing between a weapon and a weapons system. Although persons are specifically referenced, defining a combatant as a weapon or weapons system operator theoretically opens the door to AWS falling within the category of combatant. AWS seem to fall somewhere between the extant legal definitions of weapons and combatants. If they were to be simply classified as weapons, that would ignore the fact that they are not directly employed by human beings to inflict violence but that they are in a sense a weapons deployment platform that comes between the human operator and the weapon itself; it would also ignore the fact that these systems have many different levels of autonomy as to whether to deploy force or not. On the other hand, International Humanitarian Law rules that define who is and who is not a combatant seem specifically, by their discussion of types of humans, to exclude machinery. It is obvious that there are a number of theoretical and practical difficulties in defining AWS as combatants. However, if AWS are defined merely as weaponry, the systems to regulate their use will only address part of their operational capabilities, and therefore not fully deal with the significant threat such systems contain.

Due to the significant impact it would have on IHL, it is not the aim of this chapter to categorise AWS as combatants. Rather, the purpose of this section is to question the classification of AWS solely as weapons, and to cast light on the possible impact of making weapons systems autonomous.

Defining Weapon, Means of Warfare and Methods of Warfare

What is a Weapon?

The Oxford Dictionary defines weapon as 'a thing designed or used for inflicting bodily harm or physical damage; a means of gaining an advantage or defending oneself'.[524] However, in Additional Protocol I of the Geneva Convention (API), the term weapon is not defined. Furthermore, the very limited definitions provided by the 1899 Hague Declaration Concerning Expanding Bullets and the Convention on Certain Conventional Weapons- Protocols I (non-detectable fragments), II (mines, booby-traps and other devices), III (incendiary weapons) and IV (blinding laser weapons) are solely concerned with whether the restrictions identified in the

[524] *Concise Oxford Dictionary* (OUP, 2006).

relevant declaration or protocol can be applied to the weapon discussed.[525] Under the US directives, all weapons can be subject to legal review. To illustrate, a blinding laser weapon as defined in the CCW Protocol IV has been deemed to not include eye-safe lasers, which are not lethal and can only confuse those they are used on.[526]

As each department of the US military, i.e. the Army, Navy and Air Force, has a unique function, weapon is defined in three different ways in US directives that address the legal review of weapons. For the purposes of a legal review, a weapon as used by the US Army includes 'chemical weapons and all conventional arms, munitions, materiel, instruments, mechanisms, or devices which have an intended effect of injuring, destroying, or disabling enemy personnel, materiel or property.'[527] In the US Navy, a weapons system or weapon is 'all arms, munitions, materiel, instruments, mechanisms, devices and those components required for their operation, that are intended to have an effect of injuring, damaging, destroying, or disabling personnel or property, [including] non-lethal weapons. For [the] purpose of the legal review, weapons do not include launch or delivery platforms, such as, but not limited to, ships or aircraft, but rather the weapons or weapon systems contained on those platforms.'[528] Finally, the US Air Force defines a weapon as 'devices designed to kill, injure or disable people, or to damage or destroy property. Weapons do not include devices developed and used for training and practice; aircraft, intercontinental ballistic missiles, and other launch platforms; or electronic warfare devices.'[529]

The above definitions are all similar, but while the Air Force and Army definitions do not include non-lethal devices, the Navy's definition does. The US Department of Defense (DoD) has its own directive for the acquisition and development of 'less-lethal' weaponry.[530] This directive requires

[525] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts. See Dietrich Schindler & Jiri Toman (eds), *The Laws of Armed Conflicts: A Collection of Conventions, Resolutions, and Other Documents* (Brill – Nijhoff, 4th edition, 2004) 199.
[526] Dietrich Schindler & Jiri Toman (eds), *The Laws of Armed Conflicts: A Collection of Conventions, Resolutions, and Other Documents* (Brill – Nijhoff, 4th edition, 2004) 212.
[527] Result of a US Department of Defense Working Group cited in ICRC, A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977 (Geneva: ICRC, 2007) 8.
[528] Secretary of the Navy Instruction 5000.2C (19 November 2004), Subject: Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System 23.
[529] Air Force Instruction 51-402 (13 May 1994), Subject: Weapons Review 1.
[530] DoD Directive 3000.3 (9 July 1996), Subject: Policy for Non-Lethal Weapons.

that this type of weapon be subject to a Law of War review. While the DoD's Law of War Working Group has considered formulating a unified definition of weapon, the distinct tasks of different US military departments and their related weaponry has forestalled the creation of this definition.[531] Confusion can arise even when a definition is given. An attack plane may be a weapons system or a weapon. If considered a weapons system, the question then arises of whether the entire plane must be subjected to a legal review or simply the weaponry it is equipped with that is used to deliver munitions. The definitions offered by the Air Force and the Navy can clarify this and similar issues, but the Army definition cannot. Another common issue is whether an electronic device that can hinder the functioning of enemy devices temporarily should be considered a weapon despite the fact that it does not physically damage property or enemy combatants. On this issue, the Army and Navy definitions of weapons are silent, but the Air Force definition offers a resolution. However, as has been seen, complications can still emerge.

In international law, the issue becomes even more problematic, with the international legal regime providing no definition of weapon. As a result, the meaning of the word weapon 'is unclear across the international community, as each state tends to have its own definition.'[532] To illustrate, Australia defines a weapon as 'an offensive or defensive instrument of combat used to destroy, injure, defeat or threaten. [The term] includes weapon systems, munitions, submunitions, ammunition, targeting devices, and other damaging or injuring mechanisms.'[533] In Belgium, the term denotes 'any type of weapon, weapon system, projectile, munition, powder or explosive, designed to put out of combat persons and/or materiel',[534] while Norway defines a weapon as 'any means of warfare, weapons systems/ project, substance, etc. which is particularly suited for use in combat, including ammunition and similar functional parts of a weapon.'[535] Finally, to return to

[531] The International Committee of the Red Cross's 'A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977' (2006) 88 *International Review of the Red Cross* 8.
[532] ICRC, 'A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977' (2006) 88 *International Review of the Red Cross* 47.
[533] Australia: Legal Review of New Weapons, Australian Department of Defence Instruction (General) OPS 44-1 2 June 2005 Subsection 3(a) of the Australian Instruction.
[534] ICRC, 'A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977' (2006) 88 *International Review of the Red Cross* 937 (citing subsection 1(a) of Defense, Etat-Major de la Defense, Ordre General - J/836 (18 July 2002), which established La Commission d'Evaluation Juridique des nouvelles armes, des nouveaux moyens et des nouvelles methodes de guerre).
[535] ICRC, 'A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977' (2006) 88 *International Review of the Red Cross* 937 (citing subsection

the US, the US DoD Directive on the Legal Review of Non-Lethal Weapons 'defines non-lethal weapons as weapons that are explicitly designed and primarily employed so as to incapacitate personnel or materiel, while minimizing fatalities, permanent injury to personnel, and undesired damage to property and the environment.'[536]

In the US, a weapons system is defined as the 'weapon itself and those components required for its operation, including new, advanced or emerging technologies which may lead to development of weapons or weapon systems and which have significant legal and policy implications. [Weapon] systems are limited to those components or technologies having direct injury or damaging effect on people or property (including all munitions and technologies such as projectiles, small arms, mines, explosives, and all other devices and technologies that are physically destructive or injury producing)'.[537] In line with this definition, all weapons systems in the US are subject to legal review.[538]

The International Committee of the Red Cross (ICRC) and several other scholars have spoken in support of the inclusion weapons systems in Article 36.[539] Indeed, Article 36 of API offers a wider scope for the language used when compared with Article 35. Specifically, Article 36 cites 'weapons, means and method of warfare', while Article 35 refers to 'weapons, projectiles and material and methods of warfare.'[540]It is clear that the language used in this article sums up the long observed international law convention that some types of weaponry are not acceptable (ethically and morally) and so they are not permitted (normatively and legally). It must be noted that neither the Geneva Conventions nor the Additional Protocols contain a great deal of specific information regarding prohibited weapons; they rely on states making the appropriate judgements as to whether or not a weapon is prohibited. It has been suggested that the drafters of Article 36

1.4 of The Norway Ministry of Defence Directive on the Legal Review on Weapons, Methods and Means of Warfare -Direktiv om folkerettslig vurdering av vapen, krigforingsmetoder og krigforingsvirkemidler- (2003)).
[536] US DoD *Policy for Non-Lethal Weapons Directive 3000.3* para 5.6.2.
[537] William Parks, 'Office of The Judge Advocate General of the Army, Weapons Review Programme of the United States' presented at the Expert Meeting on Legal Reviews of Weapons and the SIrUS Project, Jongny sur Vevey, Switzerland, 29–31 January 2001 (on file with the ICRC).
[538] ICRC, 'A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977' (2006) *International Review of the Red Cross*.
[539] William Boothby, *Weapons and the Law of Armed Conflict* (Oxford University Press, 2009) 4.
[540] See Article 35 and 36 of Additional Protocol I.

used this language expressly to include weapons system and thus 'more than just material, projectiles, or kinetic kill vehicles.'[541]

The task of defining what constitutes a weapon has not been left solely to official bodies but has also been taken up by scholars. McClelland argues that defining the term weapon is, in fact, 'a relatively straightforward process. The term connotes an offensive capability that can be applied to a military [objective] or enemy combatant'.[542] Boothby states that a weapon can be 'a device, implement, substance, object or piece of equipment' so long as it is the means used to deliver an offensive action targeted at the enemy or delivered to achieve a military goal.[543]

Importantly, the definitions of weapon put forward by scholars and states fail to address the full scope of the term. Nonetheless, they identify three key elements of a weapon: 1) it must be capable of causing direct harm or of satisfying defensive objectives; 2) it is an object that is utilised by a subject (as evidenced by the repeated use of the words 'employed', 'used' and 'applied' in definitions; and 3) it includes weapons systems.

Yet, despite the prevalence of the explicit inclusion of weapons systems in definitions of the term weapon, commentators have criticised this understanding. A weapons system is not in truth a weapon but the stage from which a weapon is delivered. Historically, human beings have been the ones to deliver weapons. Given the changing face of warfare, it is to a certain point reasonable that some weapons systems may be deemed to be weapons themselves. This is appropriate when, for instance, the system can cause a 'direct injury or damaging effect on people or property.'

However, there is great variety among autonomous weapons systems (AWS) and these differences need to be taken into account at the beginning of the legal review of new weapons process. As discussed in the first chapter of this dissertation, there is a wide spectrum on which the autonomy of a weapons systems may find itself. The closer a weapons system is to being entirely

[541] Duncan Blake & Joseph Imburgia, 'Bloodless Weapons? The Need to Conduct Legal Reviews of Certain Capabilities and The Implications of Defining them as Weapons' (2010) 66 *Air Force Law Review* 171.
[542] Justin McClelland, 'The Review of New Weapons in Accordance with Article 36 of Additional Protocol I (2003) 850 *ICRC* 397.
[543] William Boothby, *Weapons and the Law of Armed Conflict* (OUP, 2009) 4.

autonomous, that is, able to perform its vital functions (e.g. search, kill etc.) free of any human input, the greater the complexity in determining whether it is a weapon under Article 36, and thus subject to legal review.

Implications of Weapons Autonomy for Legal Analysis

The autonomous devices of interest in the present work are those that play a significant part in armed conflicts through the application of military force. Thus, autonomous gun turrets, unmanned aerial vehicles and the like are clearly included as weapons form an integral part of these machines. Furthermore, the scope of this research includes those devices that participate in the decision to apply force. For example, an automated intelligence, surveillance and reconnaissance system that supplies data on possible targets to a distinct weapons system may be included. In sum, any autonomous system that Article 36 would describe as a means or methods of warfare or as a weapon are the focus of the present research.

The ICRC's Dr Giacca, speaking at the 2016 CCW Informal Meeting of Experts, attempted to explain the scope of the devises that the duty of legal review applies to:

'Defensive or offensive device with the capability to kill, injure, disable people and/or destroy or damage property. Ranging from rifles, plateforms, sighting equipment, laser designators, target acquisition equipment, data links and software used for processing target data all require legal review. It would also include new military doctrine that applies to weapons.'[544]

It is noteworthy that the above identifies parts of weapons systems as well as weapons platforms means of warfare. In the context of autonomous machines, this detail is significant as it suggests that AWS would be categorised as a means of warfare given that the control systems that operate these devises typically form part of a weapons platform. Alternately, the control systems are in contact with or connected to the AWS. However, this does not preclude the inclusion of an AWS in the category of 'weapon'. Again, the ICRC API commentary offers insight into this matter, highlighting that the drafters of API were aware of the issue of the automation of the battlefield:

[544] Gilles Giacca, (Notes, CCW Meeting of Experts on LAWS: Challenges to International Humanitarian Law, April 2016) 4.

'The use of long distance, remote control weapons, or weapons connected to sensors positioned in the field, leads to the automation of the battlefield in which the soldier plays an increasingly less important role. The counter-measures developed as a result of this evolution, in particular electronic jamming (or interference), exacerbates the indiscriminate character of combat. In short, all predictions agree that if man does not master technology, but allows it to master him, he will be destroyed by technology.'[545]

Two key aspects of an autonomous machine may exclude it from being defined as a weapon in a legal context. Firstly, the task achieved by the machine may affect whether it is considered a weapon. An unmanned vehicle that transports cargo using an autonomous navigation system is not a weapon, but an Unmanned Aerial Vehicle that chooses and engages targets using autonomous capabilities is. Other systems may be more difficult to classify. If an autonomous element supplies target data to a weapons platform directly, it can be considered to form part of a weapons system. However, if such an autonomous system provides data indirectly through an intermediary, whether it be mechanical or human, that then makes the final decision for combat engagement, the classification of the autonomous system is not easy to determine. The causal link between an autonomous machine and the damage or harm done to a combatant can be weaker or stronger, and thus those responsible for reviewing autonomous machines must determine whether this link is strong enough for the machine to be classed as a means of warfare or weapon. Yet, it is important to recall that the scope of the terms means of warfare and weapons is supposed to be a wide one.

Secondly, the extent of control that a human or computer has over an autonomous machine's behaviour can affect the machine's classification. As previously discussed, a human agent can control an autonomous machine in various ways and to various extents. The time and context in which the machine is controlled and the operational function utilised can all change. To illustrate, if human operators were to control an autonomous system to the point where they were acting as an intermediary between a weapons platform and the system, it is likely that the system will be

[545] Jean de Preux, 'Protocol I – Article 36-New Weapons' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 427.

deemed too distant to be considered part of the relevant weapons system and thus will not be categorised as a weapon.

Unlike weapons and means of warfare, it is doubtful that new AWS will require a legal review as regard their status as methods of warfare. Although autonomous capacity could result in the development of new combat strategies applied with the use of AWS, this will probably be considered within the legal review concerning the machine's status as a means of warfare or weapon. To conclude, there is a broad but not limitless range of autonomous machines that can be classed as a means of warfare or as a weapon.

Superfluous Injury and Unnecessary Suffering

Content of The Principle

The ban on weapons that cause unnecessary suffering, as a customary international law rule, applies within both international armed conflict (IAC) and non-international armed conflict (NIAC).[546] As such, regardless of whether a state is party to API, it has obligations under customary international law deploy munitions that cause unnecessary suffering. It is arguable, therefore, that if the characteristics of a weapon system, such as autonomous critical functions, would then mean that otherwise lawful weapons were used to inflict superfluous harm, or cause unnecessary suffering, then the system would violate a fundamental rule of international weapons law.

Numerous treaties address a ban on weapons that cause unnecessary suffering or superfluous harm. In some such treaties, this rule indicated the banning of a specific weapon. Some examples of these treaties, either implementing this rule or inspired by it, are the Geneva Gas Protocol; Additional Protocols I and II, and Amended Protocol II to the Convention on Certain Conventional Weapons; the St. Petersburg Declaration and the Hague Declarations and Regulations; the Ottawa

[546] International Humanitarian Law classifies armed conflicts as international armed conflict (IAC) or non-international armed conflict (NIAC). See Rule 70 of the ICRC Study on Customary International Humanitarian Law. The International Criminal Tribunal for the former Yugoslavia (ICTY) has confirmed the view that the principle applies not only in international but also in non-international armed conflicts. ICTY *Prosecutor v. Tadić* Decision on the defence motion for interlocutory appeal on jurisdiction Case No. IT-94-1 2 October 1995, §127.

Convention banning anti-personnel mines; and the Rome Statute.[547] Amended Protocol II to the Convention on Certain Conventional Weapons specifies its relevance for NIAC.[548] This rule is also contained within other frameworks[549] and many international conferences have made reference to it.[550]

State practice consistently supports the ban on weapons that inflict superfluous harm and cause unnecessary suffering. This ban is documented in multiple state-published military manuals,[551] with any violation considered a criminal offense.[552] This ban is also highlighted by state practice

[547] See also the ICRC 'A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977' (2006) *International Review of the Red Cross* 11.
[548] See ICRC 'A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977' (2006) *International Review of the Red Cross* 11.
[549] See Oxford Manual of Naval War, Article 16(2), 21; ICTY Statute, Article 3(a), 27; San Remo Manual, 42(a); UN Secretary-General's Bulletin, Section 6.4 p30; UNTAET Regulation No. 2000/15, Section 6(1)(b)(xx) p31; See also UN General Assembly, Res. 3076 (XXVIII), Res. 3102 (XXVIII), Res. 3255 (XXIX), Res. 31/64, Res. 32/152, Res. 33/70, Res. 34/82, Res. 35/153, Res. 36/93.
[550] See for example the 22nd International Conference of the Red Cross; 26th International Conference of the Red Cross and Red Crescent.
[551] See ICRC 'A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977' (2006) *International Review of the Red Cross* referring to the military manuals of Netherlands, New Zealand, Nigeria, Romania, Russian Federation, Senegal, South Africa, Spain, Sweden, Switzerland, Togo, United Kingdom, United States. The UK LOAC Pamphlet (1981) states: 'The following are prohibited in *international* armed conflict: … d. arms, projectiles or material intended to cause excessive injury or suffering.' United Kingdom, *The Law of Armed Conflict*, D/DAT/13/35/66, Army Code 71130 (Revised 1981), Ministry of Defence, prepared under the Direction of The Chief of the General Staff, 1981, Section 5, p. 20, § 1(d); The US Soldier's Manual (1984) states: 'The law of war does not allow you to alter your weapons in order to cause unnecessary injury or suffering to the enemy.' United States, *Your Conduct in Combat under the Law of War*, Publication No. FM 27-2, Headquarters Department of the Army, Washington, November 1984, 10; New Zealand's Military Manual (1992) provides: 'It is prohibited to employ weapons, projectiles and material of a nature to cause superfluous injury or unnecessary suffering. A weapon causes unnecessary suffering when in practice it inevitably causes injury or suffering disproportionate to its military effectiveness. In determining the military effectiveness of a weapon one looks at the primary purpose for which it was designed.' New Zealand, *Interim Law of Armed Conflict Manual*, DM 112, New Zealand Defence Force, Headquarters, Directorate of Legal Services, Wellington, November 1992, § 509(2) (land warfare) and § 616(2) (air warfare); see also §§ 510(1)(a) and 707(2) (naval warfare); South Africa's LOAC Manual (1996) states: 'A basic principle of the LOAC is the prevention of unnecessary suffering. The test in relation to a particular weapon is whether the suffering occasioned by its use is needless, superfluous, or grossly disproportionate to the advantage gained. i.Weapons which are calculated to cause unnecessary suffering are illegal per se. Such weapons include barbed spears, dum-dum bullets, weapons filled with glass and weapons that inflame wounds. ii. Legal weapons may not be used in a manner which cause unnecessary suffering'. South Africa, *Presentation on the South African Approach to International Humanitarian Law*, Appendix A, Chapter 4: International Humanitarian Law (The Law of Armed Conflict), National Defence Force, 1996, § 34(f).
[552] As above. The UNTAET Regulation No. 2000/15 establishes panels with exclusive jurisdiction over serious criminal offences, including war crimes. According to Section 6(1)(b)(xx), '[e]mploying weapons, projectiles and material and methods of warfare which are of a nature to cause superfluous injury or unnecessary suffering' constitutes a war crime in international armed conflicts. Regulation on the Establishment of Panels with Exclusive Jurisdiction over Serious Criminal Offences, UN Doc. UNTAET/REG/2000/15, Dili, 6 June 2000, Section 6(1)(b)(xx).

as being applicable to both IAC and NIAC.[553] The ban on of specific weaponry or means of warfare no longer factors on the nature of the conflict, or the adversary. As *the Tadic Case* has outlined, 'what is inhumane, and consequently proscribed, in international wars, cannot but be inhumane and inadmissible in civil strife.'[554]

The ban on weapons that cause unnecessary suffering has proven instrumental for case-law.[555] In the *Nuclear Weapons case*, for example, the court noted that this ban forms part of the 'cardinal principles' of IHL.[556] In this case, multiple parties relied on the rule.

Application to Autonomous Weapon Systems

Although the ban is widely accepted, views differ on how best to decide whether a weapon does indeed cause unnecessary suffering.[557] In the case of AWS with unpredictable performance, this consideration is particularly pertinent. It should be understood from the outset that the ban on weapons that inflict superfluous injury or cause unnecessary suffering refers to the design of the weapon. In particular, it refers to weapons that have been altered for the primary purpose of inflicting additional pain in a strike.[558]

War is, without doubt, characterised by the harm and suffering caused to combatants and non-combatants.[559] Arguably, all weapons cause suffering. However, this suffering must not be superfluous or unnecessary to achieving the military purpose for which the weapon was designed , and unnecessary harm is illegal. If a strike causes 'a great deal of suffering on enemy troops', this does not automatically constitute unnecessary levels of harm.[560] An attack becomes unlawful when

---

[553] See http://www.icrc.org/eng/war-and-law/weapons/new-weapons/overview-review-of-new-weapons.htm (accessed 1 January 2018).
[554] *Prosecutor v Tadic* IT-94-1 (1995) ICTY Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction (Appeals Chamber), para 119 and 127.
[555] *Ryuichi Shimoda et al v The State Japanese Annual of International Law (1964) 8 p 212; Military Junta case, Judgement, Argentina, National Court of Appeals*.
[556] *Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) [1996] ICJ Rep 238*.
[557] Nikolaos Sitaropoulos, 'Weapons and Superfluous Injury or Unnecessary Suffering in International Humanitarian Law: Human Pain in Time of War and the Limits of Law' (2000) *Revue Hellénique de Droit International* 108.
[558] Michael Schmitt et al, 'The Manual on the Law of Non-International Armed Conflict' (2006) *International Institute of Humanitarian Law* 12.
[559] Burrus Carnahan, 'Unnecessary Suffering, the Red Cross and Tactical Laser Weapons' (1996) 18 *Loyola International & Comparative Law Review* 773.
[560] Christopher Greenwood, 'Battlefield Laser Weapons in the Context of the Law on Conventional Weapons' in Louise Doswald-Beck (eds), *Blinding Weapons, Reports of the Meetings of Experts Convened by the International*

the suffering it causes has no military purpose.[561] Certain characteristics have been specified, that determine whether a weapon is indeed a prohibited weapon. Some of these are as follows:

It is widely agreed[562] that any suffering caused without military purpose is unlawful in accordance with the ban on means and methods of attack that inflict superfluous harm, or cause unnecessary suffering.

This ban makes it necessary for belligerents to strike a balance between their anticipated military gain and the anticipated harm they will cause. The rule is violated if the suffering or injury caused is disproportionate to the military advantage they were seeking.[563] As such, unnecessary suffering was, in *the Nuclear Case*, defined as 'harm [which is] greater than that unavoidable to achieve legitimate military objectives.'[564]

Research in this area concludes that superfluous injury and unnecessary suffering are 'design-dependent.'[565] That is to say, that the focus of this consideration must be the weapon itself *per se*. In the case of AWS, this must be very carefully considered. First, the level of discrimination and unnecessary suffering caused could greatly depend on a weapon's operator. In the case of AWS, the operator is the autonomous system. The extent to which an AWS is autonomous is thus very important when considering its legality.

Committee of the Red Cross on Battlefield Laser Weapons 1989-1991 (International Committee of the Red Cross, 1993) 71.

[561] Myres McDougal & Florentino Feliciano, *Law and Minimum World Public Order* (Yale University Press, 1961) 616.

[562] Jean de Preux, 'Protocol I – Article 35 – Basic Rules' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 400 [1411]; William Boothby, *Weapons and the Law of Armed Conflict* (Oxford University Press, 2009) 60.

[563] Humanitarian Law in Armed Conflicts – Manual, DSK VV207320067, edited by The Federal Ministry of Defence of the Federal Republic of Germany, VR II 3, August 1992, English translation of ZDv 15/2, Humanitäres Völkerrecht in bewaffneten Konflikten – Handbuch, August 1992. This manual was superseded by Law of Armed Conflict - Manual, Joint Service Regulation (ZDv) 15/2, DSK AV230100262, Federal Ministry of Defence, Berlin, 1 May 2013, English version of ZDv 15/2, Humanitäres Völkerrecht in bewaffneten Konflikten - Handbuch, 1 May 2013, 58; Military Manual (1992) Interim Law of Armed Conflict Manual, DM 112, New Zealand Defence Force, Headquarters, Directorate of Legal Services, Wellington, November 1992. 73.

[564] *Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) [1996] ICJ Rep 238.*

[565] Robin Coupland, 'Towards a Determination of Which Weapons Cause Superfluous Injury or Unnecessary Suffering' (1997) *The SIrUS Project* ICRC 8.

Historically, many weapons were considered compliant with the ban owing to the regulation around their specific operation. Although the design of the weapon may be considered lawful, it is important to note that a lawful weapon may still be used to cause unnecessary, and disproportionate suffering to the targeted adversary. For example, if a combatant employs a sniper rifle to strike a combatant's limbs one by one, then leave them to bleed out, or suffer permanent disability, they are considered to be acting unlawfully. Once an enemy combatant is incapacitated, their human opponent would cease fire. Arguably, if the circumstances suggested that an enemy combatant would soon surrender, on account of fatigue or other reasons, a human combatant would refrain from causing them any further harm. This concept of refraining from causing unnecessary harm, even in the face of a legitimate enemy, is founded on simple humanity. Individual enemy combatants are, of course, only enemies because they represent the enemy force. Rousseau rightly noted:

'War is in no way a relationship of man with man… individuals are enemies only by accident; not as men, nor even as citizens, but as soldiers . . . since the object of war is to destroy the enemy state, it is legitimate to kill the latter's defenders as long as they are carrying arms; but as soon as they lay them down and surrender, they cease to be enemies or agents of the enemy, and they again become mere men and it is no longer legitimate to take their lives.'[566]

To take the life of an individual who was injured, or to continue to injure them, would, without question, represent unnecessary suffering. Such tactics would have no military aim, and would only be employed to inflict further harm. Naturally, the final consideration of whether unnecessary harm or suffering were to be caused, would lie in the hands of the human combatant operating the weapon. It would be their responsibility to ensure the weapon were used appropriately. Human combatants are, arguably, a major factor in whether a weapon causes unnecessary harm, as they have ultimate control over its use. Retired Major General William H. Rupertus refers to the traditional relationship between a weapon and its operator, in 'My Rifle: The Creed of a US Marine': [567]

[566] JJ Rousseau quotation from Anicee Van Engeland, *Civilian or Combatant?: A Challenge for the 21st Century* (Oxford University Press, 2011) 13.

[567] '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. Without my rifle, I am useless. I must fire my rifle true...

It appears that, in the case of AWS, this creed will be sworn by the autonomous systems themselves. Humans will simply have to expect for a positive outcome. It should, as such, be considered that in view of the ban on weapons that cause unnecessary suffering, the stakes have changed where increasingly autonomous, or fully autonomous weapons are concerned. It is simply not sufficient for an AWS' weapon to be, in itself, legal. This is because a weapon alone cannot cause unnecessary suffering or superfluous injury.

In the case of AWS, the method of warfare is different. No human operator makes the responsible decision to refrain from inflicting unnecessary harm on a target, even if they are legitimate. With weapons now operated by an autonomous piece of equipment, or, as referred to above, a 'robo-combatant', despite the weaponry being legal, questions arise as to whether the combination of autonomy and lethality does indeed violate the ban on weapons that cause unnecessary suffering and superfluous injury.

This consideration is triggered by the fact that humans have intuition, whereas machines do not. As Rousseau states[568], combatants are only enemies by circumstance; as individuals, they are not enemies.

Some arguments have naturally highlighted the fact that some robots can now determine whether or not an individual is in pain. That said, it is yet to be seen whether such capability will be coded into AWS. If so, it remains to be seen whether they will be able to decide, like a human, not to cause unnecessary suffering or superfluous injury.

In this case, if AWS themselves are to be considered as weapons, they should be considered as a complete entity. That is to say, that their additional or total autonomy and lethality should be

---

My rifle is human, even as I, because it is my life. Thus, I will learn it as a brother. I will learn its weaknesses, its strength, its parts, its accessories, its sights, and its barrel. I will ever guard it against the ravages of weather and damage as I will ever guard my legs, my arms, my eyes, and my heart against damage. I will keep my rifle clean and ready. We will become part of each other. We will...Before God, I swear this creed.' See http://usmilitary.about.com/od/marines/l/blriflecreed.htm (accessed 28 January 2018).

[568]Jean-Jacques Rousseau, *1712-1778 The Essential Rousseau: The Social Contract, Discourse on the Origin of Inequality, Discourse on the Arts and Sciences, The Creed of a Savoyard Priest* (1974) New American Library 18.

combined. Contrary to the comments of Schmitt, the lethality and autonomy of an AWS should not be considered mutually exclusive. The question is, rather, whether lethal AWS could inflict unnecessary suffering or cause superfluous injury, thus constituting unlawful weapons *per se*.

To answer this question, one must not simply consider the design of the weapons themselves, but how they are employed by the AWS. In terms of the human considerations they must make—considerations which only a human can make—it is likely that AWS will be unable to meet this requirement, as stipulated by international weapons law.

When considering the legality of a weapon, it is important to consider the availability of alternatives, capable of achieving the same military effect.[569] This consideration highlights that the rule specifies the relevance of both the design and use of a weapon. As such, if a combatant has access to two different weapons that could fulfil the same military objective, they must select the weapon that will not inflict superfluous harm upon their adversary. Naturally, it is important that the alternative weapon must be easily accessible. Combatants cannot carry an entire arsenal of weapons, waiting for the appropriate opportunity to use them.[570] Carnahan therefore states that a weapon can be considered to cause unnecessary suffering when '…it is deliberately altered for the purpose of increasing the suffering it inflicts…, its military advantages are marginal…, [if it is] deliberately selected for the suffering that it inflicts when other, equally effective means are readily available.'[571]

This text, however, considers the method of warfare specifically. It considers circumstances whereby a belligerent can choose between a human operator for a weapon, or an AWS. As such, the ICRC has urged states to reflect upon the necessity of using an AWS with enhanced, or full autonomy.[572]

---

[569] Manual for Military Commissions, published in implementation of Chapter 47A of Title 10, United States Code, as amended by the Military Commissions Act of 2009, 10 U.S.C, §§ 948a, et seq., 27 April 2010 88.
[570] Antonio Cassese, 'Weapons Causing Unnecessary Suffering: Are They Prohibited?' (1975) 58 *Rivista Di Diritto Internazionale* 15.
[571] Burrus Carnahan 'Unnecessary Suffering, the Red Cross and Tactical Laser Weapons' (1996) 18 *Loyola International & Comparative Law Review* 722.
[572] International Committee of the Red Cross, 'Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centered Approach' (6 June 2019) <https://www.icrc.org/en/document/artificial-intelligenceand-machine-learning-armed-conflict-human-centred-approach> Accessed 17 February 2020.

A state may prefer to employ an AWS for multiple reasons. In particular, the increased autonomy of such platforms is unavoidable, and such platforms are typically more safe and efficient in their delivery of munitions.[573] Other reasons, however, may be considered weak, especially if they risk violating international weapons laws such as the ban on weapons that cause unnecessary suffering. As this section has discussed, and despite the fact that armed conflict permits combatants to kill, the use of weapons that imply certain death contravenes the laws of humanity, and causes superfluous harm.[574] Certain death was a key factor in the banning of poison, and expanding, exploding and 'dum-dum' bullets.[575] There are many official documents banning and condemning weapons that imply certain death.[576] These official documents clearly demonstrating states` revulsion against the concept of unnecessary suffering. It is legal to kill enemy combatants who are actively engaged in hostilities.[577] If an enemy combatant were to be incapacitated, it would then become illegal to kill said combatant.[578] Human consideration then becomes vital. However, scrutiny of the way in which AWS will identify targets greatly threatens compliance with this rule.

The ability of an AWS to analyse a situation, and changing circumstances like a human has been called into question. Arguably, if an autonomous robot is to target an individual based on facial recognition, its deployment thus marks the point at which their death is made certain. Even if circumstances were to change for that individual, this would not change. This would be the case even if they chose to surrender, or lay down their weapons.

---

[573] Ronald Arkin, 'Lethal Autonomous Systems and the Plight of the Non-combatant' in Ryan Kiggins (eds), *The Political Economy of Robots International Political Economy Series* (Palgrave Macmillan, 2018) 325.
[574] The preamble to the St. Petersburg Declaration states that the use of such weapons 'would be contrary to the laws of humanity.'
[575] Air Force Pamphlet 110-31, International Law – The Conduct of Armed Conflict and Air Operations, US Department of the Air Force, 1976 88; Air Force Commander's Handbook (1980), Air Force Pamphlet 110-34, Commander's Handbook on the Law of Armed Conflict, Judge Advocate General, US Department of the Air Force, 25 July 1980 89.
[576] See for example the military manual of Belgium Law of War Manual (1983) Droit Pénal et Disciplinaire Militaire et Droit de la Guerre, Deuxième Partie, Droit de la Guerre, Ecole Royale Militaire, par J. Maes, Chargé de cours, Avocat-général près la Cour Militaire, D/1983/1187/029, 1983, 36, Ecuador Naval Manual (1989) Aspectos Importantes del Derecho Internacional Marítimo que Deben Tener Presente los Comandantes de los Buques, Academia de Guerra Naval, 1989, 52.
[577] Anicee Van Engeland *Civilian or Combatant: A Challenge for the 21st Century* (OUP, 2011) 13.
[578] Claude Pilloud and Jean Pictet, 'Protocol I – Article 41 – Safeguard of An Enemy Hors De Combat' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 482.

Furthermore, weapon systems with enhanced autonomy or full autonomy could risk contravening the rule on avoiding collateral damage. It has been highlighted that such platforms could make it difficult or impossible to spare those who surrender.[579] In such situations, their death arguably becomes certain at the point at which the weapon system is deployed. As such, the AWS itself may be considered unlawful *per se*.

The rule is considered violated by any weapon whose use implies serious permanent disability[580] It is for this reason that anti-personnel landmines and blinding lasers are prohibited,[581] as is the used of incendiary weapons against personnel.[582] As discussed in previous sections, such weapons that do not necessarily imply permanent disability could be capable of causing such disability, depending on the actions of the operator. Traditionally, weapons did not make decisions on the time, place, and target of an attack. As such, it was sensible to assess their legality primarily in terms of their design. Now such weapons are interfaced with autonomous systems, it is arguable that their assessment should consider additional factors such as unpredictability. It is impossible to determine whether an AWS, when operating in a dynamic environment, and when employing otherwise legal weapons, would cause permanent disability.

Prohibition of Weapons Which are Indiscriminate in Nature

Content of The Principle

The principle of distinction, as one of the 'cardinal principles'[583] of IHL, specifies that all belligerents must 'at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.'[584] It thus provides specific limitations and requirements for the means and methods of warfare that belligerents may consider. This section will concentrate on the

[579] Michael Schmitt and Jeffrey Thurnher, '"Out of the Loop": Autonomous Weapon Systems and the Law of Armed Conflict' (2013) 4 *Harvard National Security Journal* 258.
[580] Air Force Commander's Handbook (1980), Air Force Pamphlet 110-34, Commander's Handbook on the Law of Armed Conflict, Judge Advocate General, US Department of the Air Force, 25 July 1980, 88.
[581] The preamble of the Ottawa Convention; France, LOAC Manual (2001) Manuel de droit des conflits armés, Ministère de la Défense, Direction des Affaires Juridiques, Sous-Direction du droit international humanitaire et du droit européen, Bureau du droit des conflits armés, 2001, 55.
[582] See Commentary to Rule 85 of ICRC Study on Customary IHL Rules.
[583] *Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)* [1996] ICJ Rep 226, 257 [78].
[584] *API* art 48.

interpretation of these limitations and requirements in the context of AWS, and the relevance of any specific limitations and requirements to these platforms.

When discussing the principle of distinction, it is important to note its two key considerations. The first is the design and characteristics of a weapon. The second is the restrictions on their use. This section will further focus on the first consideration, in relation to weapon law. Weapons cannot legally be used in a planned attack if, due to their design, they are unable to discriminate between legitimate and illegitimate targets. Such attacks are split into two categories, as detailed in Article 51(4) of API:

Indiscriminate attacks are:

…

(b) Those which employ a method or means of combat which cannot be directed at a specific military objective; or

(c) Those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol;

Weapons used in the first kind of attack are considered illegal due to their inability to comply with the rule of distinction, and cannot be used with sufficient accuracy in the specific circumstances for which their used was intended.[585] API prohibits indiscriminate attacks, describing them as '[t]hose which employ a method or means of combat which cannot be directed at a specific military objective.'[586] A suitable and relevant example of such a weapon would be a long-range missile with very little guidance, meaning that its final destination is difficult to adequately determine. Two such missiles are the German V1 and V2 rockets used at the end of WWII, as discussed by the ICRC commentary on the Additional Protocols to the Geneva Conventions.[587]

[585] Michael Schmitt, 'The Principle of Discrimination in 21st Century Warfare' (1999) 2 *Yale Human Rights and Development Journal* 143, 147.
[586] *API* art 51(4)(b)
[587] Claude Pilloud and Jean Pictet, 'Protocol I – Article 51 – Protection of the Civilian Population' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (Martinus Nijhoff Publishers, 1987) 613, 621; Stuart Casey-Maslen and Sharon Weill, 'The Use of Weapons in Armed Conflict' in Stuart Casey-Maslen (ed), *Weapons Under International Human Rights Law* (Cambridge University Press, 2014) 248.

Naturally, sufficient accuracy cannot be measured. Whilst some weapons are more likely to behave in an indiscriminate manner, there is no clear distinction between those which are inherently indiscriminate, and those which are not. The assessment of their ability to discriminate is contextual. It considers whether the weapon is capable of behaving discriminately, based on its intended application, and the scenarios within which it may be employed.[588] The ability of a weapon to discriminate is sometimes debatable. Mines and cluster munitions, for example, divide opinion. Mines and cluster munitions are prime examples of weapons that cause indiscriminate harm, and have been banned by many states.[589] Nevertheless, both weapons could, in specific circumstances, be employed in a manner than is legally compliant.[590] In order for their use to be considered legal, it would have to be appropriately restricted. [591] Another example of indiscriminate weapons is Scud missiles used by Iraq in 1991.[592] As 'highly inaccurate theater ballistic missiles', Scuds 'can cause extensive collateral damage well out of proportion to military results.'[593] The used of Scud missiles against Israeli and Saudi cities was widely considered to be indiscriminate.[594] Nevertheless, Scud missiles can, in some circumstances, be employed in a discriminate manner: 'For example, if employed in the vast expanses of the desert against troops,

[588] William Boothby, *Weapons and the Law of Armed Conflict* (Oxford University Press, 2009) 1.
[589] Preamble 'Weapons which may be deemed to be excessively injurious or to have indiscriminate effects, and calling for the early ratification of this Protocol by all States which have not yet done so.' United Nations, *Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on Their Destruction*, 18 September 1997 *Ottawa Convention*, *Cluster Munitions Convention*.
[590] *Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices as amended on 3 May 1996 (Protocol II, as amended on 3 May 1996) annexed to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to have Indiscriminate Effects*, opened for signature 3 May 1996, 2048 UNTS 93 (entered into force 3 December 1998) ('*CCW Protocol II*'); Secretary of Defense, 'DoD Policy on Cluster Munitions and Unintended Harm to Civilians' (Memorandum, United States Department of Defense, 19 June 2008) <http://www.acq.osd.mil/tc/treaties/ccwapl/DoD%20Policy%20on%20Cluster%20Munitions.pdf>.
[591] For a general discussion of *CCW Protocol II* (albeit prior to the 1996 amendment) see APV Rogers, 'A Commentary on the Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices' (1987) 26 *Military Law and Law of War Review* 185; Burrus Carnahan, 'The Law of Land Mine Warfare: Protocol II to the United Nations Convention on Certain Conventional Weapons' (1984) 105 *Military Law Review* 73; PJ Ekberg, 'Remotely Delivered Landmines and International Law' (1995) 33 *Columbia Journal of Transnational Law* 149.
[592] Eitan Barak (ed), *Deadly Metal Rain: The Legality of Flechette Weapons in International Law* (Martinus Nijhoff, 2011) 210.
[593] United States Department of Defense 'Report to Congress on International Policies and Procedures Regarding the Protection of Natural and Cultural Resources During Times of War' (19 January 1993) reproduced in: Patrick J Boylan *Review of the Convention for the Protection of Cultural Property in the Event of Armed Conflict* (UNESCO, 1993) 203 <http://unesdoc.unesco.org/images/0010/001001/100159eo.pdf>.
[594] Michael Schmitt, 'Future War and the Principle of Discrimination' (1999) 28 *Israel Yearbook on Human Rights* 55.

military equipment, or bases far removed from population centers, little danger of random destruction of protected persons or objects exists.'[595]

Weapons used in the second type of attack outlined by Article 51(4) of API are considered illegal as their effects cannot be controlled sufficiently to ensure they strike only military targets. It considered such weapons to be 'those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.'[596] Whilst the first type of illegal weapon is banned because it cannot sufficiently discriminate between legitimate and illegitimate targets, this second type is banned because it cannot limit its effects to the target. The words, 'as required by this Protocol' demonstrate that such effects include any effects which would be addressed by other articles of API. Such articles include: Articles 35(3) and 55, banning 'widespread, long-term and severe damage to the natural environment', demonstrating that a weapon's immediate effects are not the only ones considered; Article 56, banning attacks on dams, dykes and further 'works and installations containing dangerous forces', demonstrates that a weapon's subsequent effects are also relevant; Articles 51(5)(b) and 57(2)(a), ban weapons which would violate the principle of proportionality and inflict excessive damage.

Bacteriological weapons are the example of a weapon banned by Article 51(4)(c). This is because, regardless of the accuracy with which a bacteriological substance is delivered to a target, it is impossible to limit the range of its impact. Such weapons cannot, therefore, be controlled in accordance with IHL. Another such example is the poisoning of drinking water.

Application to Autonomous Weapons Systems

Whilst autonomy may be relevant in some cases, the ban on weapons with unregulatable effects is not closely linked to this issue. More specifically, the ban refers to the methods by which a weapon system inflicts damage upon its target, such as the specific payload it carries.[597] Autonomy refers

[595] Michael Schmitt, 'The Principle of Discrimination in 21st Century Warfare' (1999) 2 *Yale Human Rights and Development Journal* 148.
[596] *API* art 51(4)(c)
[597] Claude Pilloud and Jean Pictet, 'Protocol I – Article 51 – Protection of the Civilian Population' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (Martinus Nijhoff Publishers, 1987) 613, 621; Stuart Casey-Maslen

to control of the weapon, rather than control of its effects. As such, a lack of control over the effects of any autonomous weapon is, at best, considered as an inability of the operator to guide a weapon onto a given military target.

The emphasis, in this case, is on the need for operators to be able to direct weapons at pre-determined military objectives, as outlined in API Article 51(4)(b).[598] This regulation refers specifically to a weapon system's specification, and provides only a minimum standard: 'International Humanitarian Law mandates no specific degree of accuracy in either weapons or tactics; it simply bars those that cannot be aimed';[599] 'it would seem clear that weapons must be capable of direction at individual military objectives and that this requirement must be understood in the context of the attack.'[600] The law is violated when an operator employs a weapon system that has not been specifically designed to discriminate between targets and non-targets.

By enabling AWS to independently identify targets, one stage of the weapon's operation is taken away from the human operator, and programmed into the control system. Legal requirements for weaponeering that would otherwise be interpreted as guidance for weapon use, such as identification of legitimate targets, instead refer to the weapon system specifications. As specific weaponeering stages are programmed into the AWS control system, weapon system operators lose responsibility for these stages, and they become engrained in the coded behaviour of the weapon system. Whilst human operation of a weapon is governed by targeting law, the coded behaviour of a weapon is governed by weapons law. This raises several new legal questions. These must all be considered when an AWS is assessed against the minimum standard outlined in API Article 51(4)(b).

To assess the legality of an AWS, a general notion of accuracy must be applied. This notion must consider a weapon's target selection, rather than just its traditional, physical accuracy. This is a

---

and Sharon Weill, 'The Use of Weapons in Armed Conflict' in Stuart Casey-Maslen (ed), *Weapons Under International Human Rights Law* (Cambridge University Press, 2014) 248.

[598] Article 51 Protection of the civilian population
4. Indiscriminate attacks are prohibited. Indiscriminate attacks are:
(b) those which employ a method or means of combat which cannot be directed at a specific military objective.

[599] Michael Schmitt, *Essays on Law and War at the Fault Lines* (T M C Asser Press, 2012) 115.

[600] William Boothby, *Weapons and the Law of Armed Conflict* (Oxford University Press, 2009) 79.

new concept within the accuracy debate, and could be considered counterintuitive, especially if an AWS is considered to replace a human soldier. This concept is, however, in keeping with the idea of in-built control, providing autonomy to weapon systems. The key legal concern in this case, is whether a weapon can be directed onto a pre-determined military target, and to what extent its effects can be limited, to avoid collateral damage. This implies a necessary level of accuracy, not just in the behaviour of its final component, but through the entire operation of the weapon, starting with target selection.

In order to direct a weapon, the operator must restrict the target boundaries until they are sufficiently certain that only the specified target will be hit, thus limiting collateral damage. This process comprises a series of actions, including selection of the target, weapon system, and time and location of weapon activation, as well as the organisation of human supervision and intervention measures, and so forth. It is further controlled through the behaviours of the weapon itself, such as sensor performance, targeting systems used, weapon specifications, and chosen payload. As one of the principles of war, distinction mandates that operator actions and weapon system behaviours must, together, specify a legitimate target, and achieve legal conditions for its attack; the weapon system must behave in such a way that only the specified target is attacked.
When traditional, unguided weapons such as rifles or artillery are employed, targeteers and weapon system operators hold complete responsibility for guiding the weapon onto a legal target. Traditionally, this would be achieved by moving the weapon into such a position that it can be operated in circumstances where the operator is sufficiently certain that a legal target is present. In these cases, the operator may not have specified an individual target, such as an enemy combatant. As such, the weapon is not limited to one specific target. Instead, it is limited to whichever targets are present at the moment in which the round or munition arrives at its intended destination. Therefore, in these instances, the weapon is not required to fire upon a pre-determined target, but to fire upon a specific time and location, with the requisite accuracy. In the case of precision-guided munitions, this location is specified by lasers, GPS, or other such precision guidance. A weapon's accuracy is measured by the extent to which it can limit the final destination area of its

projectile. For manual weapons, this accuracy is generally recorded as a 'circular error probable' (CEP).[601]

If the target selection process is predominantly conducted by the weapon's own control system, task sharing between the weapon and its operator is remodelled. In the case of missile-defence systems such as the Phalanx CIWS or the Israeli Iron Dome, the operator retains control of the time and location element, but this is controlled much more loosely than it would be for unguided weapons. In this case, operators control only the space and time in which targets can be attacked, rather than guiding the munitions to a specific location, at a specific time, whereby known targets are expected to be found. Once the space and time is fixed, the weapon control system takes command, and further discriminates targets, using radar signatures to identify threats, such as incoming missiles. The missile's in-built fire and control system takes aim, and launches the projectile. As such, a weapon's accuracy is measured according to two factors: how successful it is in determining whether an object is within its pre-programmed target list, and, once it has identified a target, the precision with which it can strike it.

These concepts are equally applicable to potential future autonomous weapon systems. In every case, an operator or attack planner will indicate the intention to strike a target, or set of targets. This could be a single target, a set of targets, all objects within a specific area that meet certain criteria, or any other given parameters. The operator will then activate an AWS, which could have more autonomy than current technologies, such as greater range or endurance, increased adaptability to new circumstances, or more complex target reasoning. Regardless, future AWS will still have certain limitations in terms of range and endurance. The legal responsibility of an attacker to strike only legitimate targets will remain extant. Whilst ensuring this legal requirement is met, the tasks allocated to a weapon system will slowly increase.

Provided an operator can limit the targets chosen by a weapon system to such an extent that it is certain to only strike legitimate targets, the weapon system will meet the minimum standard

[601] William Nelson, 'Use of Circular Error Probability in Target Detection' (Technical Report, MITRE Corporation, May 1988) <http://www.dtic.mil/dtic/tr/fulltext/u2/a199190.pdf>.

specified in API Article 51(4)(b). The operator should, more specifically, assess the two following variables:

1. To what extent the weapon's targeting system can discriminate between legitimate and non-legitimate targets, given the circumstances surrounding an attack. This variable concerns the targeting system's capabilities. This variable could, in some cases, lead to several further considerations, such as to what extent the targeting system can discriminate between combatants and non-combatants. Furthermore, operators could consider its discrimination between combatants and those who are *hors de combat*. They could also consider its ability to identify the civilian or military use of a given facility. Naturally, attack planners will question the ability of an AWS to identify the precise target (or nature thereof) that had been pre-selected by the planners. This, however, exceeds the minimum legal requirements stipulated in Article 51(4)(b).

2. To what extent a selected target can be struck. This variable concerns the weapon's performance, and is equally applicable to manual and traditional weapon systems.

If a weapon system can provide an adequate measure of accuracy, both in terms of target identification and performance, and the effects of the weapon are not unregulatable, then the weapon satisfies the weapons law elements of the State's obligation to strike only legitimate targets.

Whilst it may seem appealing for certain legal obligations to be taken on by the weapon system, such as the obligation to take all possible measures to ensure targets are legitimate[602], this will not be the case. If it were, it could be assumed that the standard applied to such obligations would then also apply to an AWS' in-built targeting system. That is to say, an AWS' software would, in any given circumstances, need to be capable of taking all possible measures to ensure targets were legitimate[603]. AWS targeting software is subject to the same standard that is applied to any other weapon's in-built software. In collateral damage assessment, it is the responsibility of 'those who plan or decide upon an attack', to '[t]ake all feasible precautions in the choice of means and

[602] *API* art 57(2)(a)(i).

[603] Claude Pilloud and Jean Pictet, 'Protocol I – Article 57 – Precautions in Attack' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (Martinus Nijhoff Publishers, 1987) 681.

methods of attack'[604]. The adequacy of such software to perform this duty is to be assessed by the attack planners, in consideration of the specific circumstances.

Plans for future AWS hint at the weapon systems having some low-level tasks encoded into them, relating to these legal obligations. The development of new technology does not, however, change the legal framework governing warfare. If an AWS has any level of in-built targeting ability, such functionality must meet the standard set by weapons law rules on target distinction. In seeking to meet their obligations, attack planners will amend their processes accordingly, ensuring that all AWS-enabled attacks are compliant with the State's obligations under international humanitarian law (IHL).

Protected Persons and Objects

If the in-built targeting functions of an AWS are to prompt reconsideration of the concepts of accuracy and distinction, so too should they prompt consideration of incidents in which an AWS destroys or harms a protected person or object. Such objects could include medical facilities, civilians, civilian objects, or medical or religious personnel. Hypothetical concerns about AWS firing upon protected persons are frequently cited by the technology's opponents, with such incidents being termed 'indiscriminate attacks.'[605] AWS adversaries use such concerns to suggest that AWS are unable to comply with IHL. What should be considered in this case, is whether an AWS firing upon a protected person or object would necessarily constitute a violation of the principle of distinction. In this instance, there are a number of potential factors which could cause a protected person or object to be harmed by an AWS. Whilst some of these factors are specific to the characteristics of AWS, some are the same as those that affect other weapon systems. Arguably, all such factors are considered by existing law, and no single factor proposes AWS as unfit for use in legal armed conflict.

Harm to protected persons is legally characterised according to its causal circumstances. The potential causes for such harm can be classified according to the three top-level components of an AWS: its human operator who activates it; its in-built targeting system; and the weapon itself. The

[604] *API* art 57(2)(a)(ii).
[605] For examples and an assessment of the arguments Armin Krishnan, *Killer Robots: Legality and Ethicality of Autonomous Weapons* (Ashgate, 2009) 98.

behaviour of the weapon itself and of its operator are considered no differently to those of a manual weapon system. As such, instances of deliberate violation of API Article 51(4)(b) [606] by the operator, an operator's negligent activation of an AWS in unsuitable circumstances, or the weapon's inability to hit a target due to poor accuracy are, thus, no different, and irrelevant to this debate. The variable which is relevant to the discussion is an AWS' in-built targeting system. Still, this functionality does not constitute a relevant factor if the weapon or operator is at fault. As such, even these cases may be considered in the same way as comparable situations using manual weaponry.

It is possible that an AWS could suffer a genuine malfunction, experience an unforeseeable or inadvertent software or hardware failure, and cause abnormal behaviours in its targeting system, prompting the weapon to fire upon a protected target. It is not yet considered that such a malfunction would have any legal implications, other than those that would be caused by a similar fault in a manual weapon system.

One remaining possibility is that an AWS could intentionally strike a protected target. That is to say, that the AWS may direct its weapon toward a protected target, in accordance with its targeting code, but against its operator's intentions. For this to happen, three potential circumstances have been identified by the current author. The first is a case whereby the AWS calculates the proportionality of a strike, and fires based upon its understanding that any ensuing civilian harm, in the given circumstances, is justified. Collateral damage resulting from AWS-conducted proportionality calculations, is legally no different than that resulting from calculations conducted by human combatants. An AWS in-built algorithm, according to which proportionality calculations are conducted, are, after all, representative of a human decision-making process.

The second cause is a case whereby an AWS is maliciously programmed to fire upon a civilian, whether by the developer, by the enemy, or by another party. Legally, this incident would, again, be no different than if another guided weapon system were compromised in the same way. Such

[606] Article 51 Protection of the civilian population
4. Indiscriminate attacks are prohibited. Indiscriminate attacks are:
(b) those which employ a method or means of combat which cannot be directed at a specific military objective

an act could constitute sabotage, an indiscriminate attack under API Article 51(4)(a), or another failure, depending on the perpetrator.

Finally, the AWS developer or other operator could unintentionally misconfigure the weapon system prior to operation, causing the in-built targeting system to mistake a civilian for a legitimate target. Such misuse is not specific to AWS, but is considered human error.[607] In this case, the individual who misconfigured the weapon system could be considered accountable for the incident, or it could be attributed to a failing in the review process established for the weapon system.

To summarise, any circumstances which could result in an AWS striking a civilian target are considered comparable to failures that could occur in any other weapon system. There appears to be no reason for AWS failures to be considered any differently. Furthermore, there appear to be no possible failures that are specific to AWS, or to which existing weapon systems law would not apply. Any malicious use of an AWS by its developer, operator, enemies, or others, would maintain the same legal character as it would if it involved another type of weapon. If civilian harm occurs, but is not caused by a deliberate act by any person, such harm constitutes collateral damage.

Conclusion

First, it is important to clearly delineate between international weapon laws, which relate to the prohibition of weapons that can kill without discrimination and cause unnecessary deaths or injuries, and International Humanitarian Law (IHL), which focuses on rules of distinction and proportionality in terms of those who use the weapons. While these rules are related to each other, they are very distinct. According to IHL, the rules of distinction and proportionality are only applicable in situations in which the international community deliberately decides to accept autonomous weapon systems as "robo-combatants" because any decisions related to who dies and

[607] Jann Kleffner, 'From 'Belligerents' to 'Fighters' and Civilians Directly Participating in Hostilities – On the Principle of Distinction in Non-International Armed Conflicts One Hundred Years After the Second Hague Peace Conference' (2007) 54 *Netherlands International Law Review* 315.

the determination of whether an act is within the confines of the law firmly belongs in the human domain.

Second, international weapons laws that prohibit indiscriminate weapons and those that can cause unnecessary harm often require an evaluation of the legality of a given weapon within the context of the weapon design. As Boothby pointed out, in light of the technologies that are available in the contemporary world, in particular those related to autonomous weapon systems, it is critical that user factors are taken into consideration when evaluating the extent in which a weapon is lawful. AWS combine two key features: Potentially lethal weapons and the ability to act autonomously. Making a decision as to the extent to which a system is lawful involves taking the autonomy and lethality of the system as an entity into consideration. When viewed in this way, AWS that have a high level of autonomy or even partial autonomy may not operate within the scope of the international weapon customary rules related to the prohibition of weapons that have the ability to act indiscriminately and/or can cause unnecessary harm.

Chapter 5 - Autonomous Weapon Systems and Legal Review of New Weapons

Introduction

Article 36 of Additional Protocol I of the 1949 Geneva Conventions clearly indicates that states have an obligation to conduct legal reviews of all new weapons, means, and methods of warfare, and to determine the legality of the weapons in some or all circumstances. As a new phenomenon in warfare, there is a need to carry out a review of autonomous weapon systems. In this chapter, I examine the problem of how effectively are states currently conducting legal reviews? In order to reveal the problem substantive analysis of State practice and *opinio juris* will be conducted.

The Legal Obligation to Conduct Legal Reviews of New Weapons

Customary and treaty law oblige states to conduct a legal review of new weapons.

Customary Law

The International Court of Justice points out that the obligation to conduct legal reviews is applicable to 'all kinds of weapons…those of the present and those of the future'.[608] Similarly, the Tokyo District Court also recognised that the IHL's principles were violated not only when the United States' dropped atomic bombs on Hiroshima and Nagasaki in World War Two, but also when the Americans failed to legally review the weapons before their use.[609]

States which are not party to Additional Protocol I of the 1949 Geneva Conventions still might recognise the obligation to review the legality of weapons under customary international law.[610] For example, the US has not ratified treaties that include this obligation, yet it reviews all new weapons in accordance with customary law requirements[611] such as those systematized in military

[608] *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion* (1996) ICJ 226,254, 259, 262.
[609] Hanrei Jiho, '*Shimoda v State of Japan'* (1964) 8 *Japanese Annual of International Law* 242.
[610] William Parks, 'Conventional Weapons and Weapons Reviews' (2005) 8 *Yearbook of International Humanitarian Law* 55; Duncan Blake & Joseph Imburgia, 'Bloodless Weapons? The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining them as Weapons' (2010) 66 *Air Force Law Review* 164.
[611] William Parks, 'Joint Service Shotgun Program' (1997) *Army Law* 16.

regulations.[612] Many scholars recognise that some states conduct legal reviews of new weapons in a customary manner, without being bound by a treaty to do so. [613]

Treaty Law

The St. Petersburg Declaration of 1868 was the first international document that clearly addressed the development of new weapons technologies. In part, it stated:

'The Contracting or acceding parties reserve to themselves to come hereafter to an understanding whenever a precise proposition shall be drawn up in view of future improvements which science may effect in the armament of troops in order to maintain the principles which they have established, and to conciliate the necessities of war with the laws of humanity.'[614]

The contemporary legal instrument that concerns the review of weapons is Article 36 of Additional Protocol I to the Geneva Conventions. It noted as follows:

'In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.'

There are two differences between the St. Petersburg and Geneva legal instruments: first, the scope of the St. Petersburg Declaration's provision is far broader than Article 36; and second, Article 36 explicitly obliges members to undertake a legal review with a preventative approach, while the St. Petersburg Declaration imposes no such obligation.

---

[612] US DoN 'Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System' (2004) *Secretary of the Navy Instruction 5000.2c* para. 2.6.2; US DoD 'The Defense Acquisition System' (2003) *Dir. 5000.01* para e1.1.1; US DoF 'Weapons review' (1994) *Instruction 51-504*; US DoA 'Review of Legality of Weapons under International Law' (1979) *Regulation 27-53* para 3.a.

[613] William Parks, 'Conventional Weapons and Weapons Reviews' (2005) 8 *Yearbook of International Humanitarian Law* 55; Michael Matheson, 'The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions' (1987) 2 *Amsterdam University Journal of International Law and Policy* 419, 420; Duncan Blake & Joseph Imburgia, 'Bloodless Weapons? The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining them as Weapons' (2010) 66 *Air Force Law Review* 163.

[614] Declaration Renouncing the 'Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, St. Petersburg, 29 November / 11 December 1868.

The ICRC indicates that Article 36 of API 'implies the obligation to establish internal procedures for the purposes of elucidating the issue of legality, and other contracting parties can ask to be informed on this point'.[615] In addition, the Red Cross and the Red Crescent argued the importance of determining the judgments, machineries and procedures which enable states to conduct legal reviews of new weapons, and to determine their legality in advance[616].

The obligation to legally review new weapons is especially important in an age when advanced military technology increasingly dominates warfare. The proliferation of advanced weaponry is harming civilians and adding unnecessary suffering to combatants. While the binding nature of Article 36 applies to all states, whether they are party or not to Additional Protocol I, [617] only a limited number of states possess mechanisms and procedures to legally review weapons, including the US[618], Norway[619], Belgium[620], Sweden[621], Australia,[622] and the Netherlands.[623]

Article 36 Scope of Application

Interpreting Article 36 can be problematic. Because Article 36 of Additional Protocol I concerns international armed conflicts, some have asked whether its obligations could be applied to weapons

[615] Y Sandoz et al, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, (ICRC, Geneva, 1987) para 1470 and 1482.
[616] The 27th and 28th International Conferences of 1999 and 2003 respectively available at https://www.icrc.org/eng/assets/files/other/icrc0021103.pdf p.20 (accessed 29 November 2017).
[617] ICRC, 'A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977' (2006) 88 *International Review of the Red Cross* 933.
[618] The US 2004 Department of Navy, Secretary of the Navy Instruction 5000.2C on Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System; The 2003 US Department of Defense Directive 5000.1 on the Defense Acquisition System; The US 1996 Department of Defense Directive Policy for Non-Lethal Weapons (3000.3); The US 1994 Weapons Review, US Department of Air Force Instruction (51-402); The US 1979 Department of Army Regulation 27-53, Regulation Legal Services: Review of Legality of Weapons under International Law and The US 1974 Review of Legality of Weapons under International Law, US Department of Defense Instruction (5500.15).
[619] The 2003 Norway Ministry of Defence Directive on the Legal Review on Weapons, Methods and Means of Warfare (Direktiv om folkerettslig vurdering av vapen, krigforingsmetoder og krigforingsvirkemidler).
[620] The Belgian 2002 Committee for the Legal Review of New Weapons, New Means and New Methods of Warfare (La Commission d'Evaluation Juridique des nouvelles armes, des nouveaux moyens et des nouvelles méthodes de guerre. Défense, Etat-Major de la Défense, Ordre Général - J/836).
[621] The Swedish Ordinance on International Law Review of Arms Projects, Swedish Code of Statutes, SFS 1994:536. (Förordning om folkrättslig granskning av vapenproject).
[622] The 2005 Australian Department of Defence Instruction on Legal Review of New Weapons (OPS 44-1).
[623] The 1978 Directive of the Minister of Defence (nr. 458.614/A) establishing the Committee for International Law and the Use of Conventional Weapons. (Beschikking van de Minister van Defensie, Adviescommissie Internationaal Recht en Conventioneel Wapengebruik).

designed for non-international armed conflict. The ICRC has stated that 'most of the [IHL] rules apply to all types of armed conflict'.[624] Likewise, in the *Tadic* case, the International Criminal Tribunal for the former Yugoslavia observed that 'what is inhumane, and consequently proscribed, in international wars, cannot but be inhumane and inadmissible in civil strife'.[625] Similarly, the Hague Declaration meetings on 'expanding bullets' have highlighted the fact that states have banned the expansion of bullets in international armed conflicts and that expanding bullets are 'in contrast to the human soul' if they are used in non-international armed conflict.[626] The valid argument is that states must therefore conduct legal reviews of new weapons as indicated in Article 36. Simultaneously, this obligation includes weapons for use in both international and domestic armed conflicts. This interpretation is important in the case of autonomous weapon systems being used to hunt terrorists in non-international armed conflict.

States should, therefore, carefully conduct legal reviews of new weapons. According to Blake and Imburgia, the scope of a legal review must be under the definition of a weapon or means of warfare.[627] It means that weapons under state control or weapons under development must be reviewed according to Article 36, but Blake and Imburgia have argued that the concept of weapons under state control must be understood to be 'the employment of weapons…the mere possession does not technically trigger Article 36 requirements'.[628] I believe that the obligation to legally review new weapons should be contained lethal, non-lethal, anti-personal, the material use of weapons, and at every stage of the possession of weapons, such as research, modification, development, purchase, and procurement.[629] If a state becomes a party to the treaty, the state should then be

[624] ICRC, 'A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977' (2006) 88 *International Review of the Red Cross* 934.
[625] *Prosecutor v Tadic Case No IT-94-1-I Decision on Defence Motion for Interlocutory Appeal on Jurisdiction*, para 119, 127 (ICTY) (2 October 1995).
[626] William Crozier, Report to the United States' Delegation to the First Hague Conference on the Proceedings of the First Commission and its Sub-Commission, July 31, 1899, referred to in Robin Coupland & Dominique Loye, 'The 1899 Hague Declaration Concerning Expanding Bullets: A Treaty Effective for More Than 100 Years Faces Complex Contemporary Issues' (2003) 849 *International Review of the Red Cross* 135, 137.
[627] Duncan Blake & Joseph Imburgia, 'Bloodless Weapons? The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining them as Weapons' (2010) 66 *Air Force Law Review* 168.
[628] Duncan Blake & Joseph Imburgia, 'Bloodless weapons? The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining them as Weapons' (2010) 66 *Air Force Law Review* 168.
[629] ICRC, 'A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977' (2006) 88 *International Review of the Red Cross* 937.

legally bound to review the weapons under its control. In essence, 'that legal review should be conducted when [a] weapon is being studied or acquired'.[630]

Some authors have observed that Article 36 is an illustration of careful examination of new weapons.[631] However, Article 36 does not provide any guidance regarding how a state conducts a legal review.[632] As a result, a review procedure should be constituted by states under their international obligations. Due to the revolutionary perspective of Article 36, evolutive interpretation and review are required when a state controls the legality or expected use of weapons and methods of warfare.[633] The revolutionary perspective is a consequence of the acquisition, modification or development of old weapons. In essence, Article 36 creates two duties on states and Lawand notes that:

'The obligation to review the legality of new weapons implies at least two things. First, a state should have in place some form of permanent procedure to that effect, in other words a standing mechanism that can be automatically activated at any time that a state is developing or acquiring a new weapon. Second, for the authority responsible for developing or acquiring new weapons, such a procedure should be made mandatory, by law or by administrative directive.'[634]

The second duty may be publicly available to the international community for close examination. Obviously, transparency of the first duty depends on the discretion of the individual state.[635] In fact, Article 36 does not require states 'to assess publicly the legality of new weapons,'[636] although

[630] James Fry, 'Contextualized Legal Reviews for the Means and Methods of Warfare: Cave Combat and International Humanitarian Law' (2006) 44 *Columbia Journal of Transnational Law* 453.
[631] Peter Ekberg, 'Remotely Delivered Landmines and International Law' (1995) 33 *Columbia Journal of Transnational Law* 149, 178 (concluding that Article 36 'implies the duty for at least a rigorous analysis of the use of remotely delivered landmines').
[632] Isabella Daoust et al, 'New Wars, New Weapons? The Obligation of States to Assess the Legality of Means and Methods of Warfare' (2002) 84 *International Review of the Red Cross* 345, 348.
[633] Christopher Greenwood, 'Customary Law Status of the 1977 Geneva Protocols' in Astrid Delissen & Gerard Tanja (eds), *Humanitarian Law of Armed Conflict: Challenges Ahead* (Martinus Nijhoff, 1991) 105.
[634] Kathleen Lawand, 'Reviewing the Legality of New Weapons, Mean and Methods of Warfare' (2006) 88 *International Review of the Red Cross* 926.
[635] Antonio Cassese, 'Means of Warfare: The Traditional and the New Law' in Antonio Cassese (eds), *The New Humanitarian Law of Armed* Conflict (Oceana Pubns, 1979) 161, 178.
[636] Jean de Preux, 'Article 36-New Weapons' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 421, 423.

it indicates that states must have internal procedures in place. Confidentiality is acceptable, however, because making information regarding the effectiveness, performance and characteristics of weapons public would give an advantage to enemy states.[637] Nevertheless, if a state fails to complete a legal review of an illegal weapon, then that state should be responsible for the possible damage the illegal weapon causes.[638]

Commentators have also asked whether, according to Article 36, states need to determine the legality of the 'normal use of a weapon as anticipated at the time of evaluation'[639] or all expected uses of a weapon or method of warfare. The rapporteur for Committee III of the diplomatic conference backs the first interpretation:

'It should also be noted that [Article 36] is intended to require states to analyse whether the employment of a weapon for its normal or expected use would be prohibited under some or all circumstances. A state is not required to foresee or analyse all possible misuses of a weapon, for almost any weapon can be misused in ways that would be prohibited.'[640]

For instance, the IHL prohibits serrated-edged bayonets because their use as an anti-personal weapon can cause unnecessary suffering.[641] Even so, some states equip their troops with these blades for digging and cutting.[642] This example clearly shows the difficulty of banning implements that might serve two or more purposes when one is deemed legal and the other/s illegal.

---

[637] Jane Gilliland, 'Submarines and Targets: Suggestions for New Codified Rules of Submarine Warfare' (1985) 73 *The Georgetown Law Journal* 975, 1002.
[638] Jean de Preux, 'Article 36-New Weapons' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 423.
[639] Jean de Preux, 'Article 36-New Weapons' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 423.
[640] Report to Third Committee on the Work of the Working Group Committee III CDDH/III/293 in Howard Levie, *Protection of War Victims: Protocol I to the 1949 Geneva Conventions* (Oceana Publications, 1980) 287.
[641] Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law* (ICRC/Cambridge University Press, 2005) Rules 70 and 71, 243.
[642] Jared Silberman, 'Non-Lethal Weaponry and Non-Proliferation' (2005) 19 *Notre Dame Journal of Law, Ethics & Public Policy* 352.

The statement 'in some or all circumstances' evidently does not oblige states to predict all expected uses of a weapon or method of warfare. However, the phrase demonstrates that the commentators are failing to properly interpret Article 36. In fact, 'in some or all circumstances' and the rapporteur's comment indicate that the legal review must simultaneously analyse the expected and normal use of weapons. Unfortunately, states prefer to give weight to the narrower interpretation of Article 36 when formulating their review procedure.

Commentators have argued that the combination of 'or' in 'in some or all circumstances' means these options are elective, and states are free to choose if their legal reviews of weapons pertain to 'some' or 'all' circumstances. The latter option is not difficult to apply because more detailed review can be caused accompanying costs to states.[643] From my point of view, the use of 'or' is similar to the use of 'and', not an alternative. Furthermore, this interpretation is promoted by the other appearance of 'or' in the Article: 'be prohibited by this Protocol *or* by any other rule of international law applicable to the High Contracting Party.'[644] Consequently, the meaning of 'or' is not optional when determining the legality of a weapon or method of warfare. A weapon's compatibility with all of a state's international legal obligations should be taken into account by a state that is party to the First Additional Protocol.[645] This interpretation of 'or' here is in line with the practice of some states (such as Australia) detecting that its legal reviews 'both with regard to provisions of Protocol I, and with regard to any other rule of international law.'[646]

During the diplomatic conference, the delegate from Mexico stated that 'it was deplorable that so far, those principles (set forth in Draft Article 33, now Article 36) had had no logical consequences at the international level in respect of existing weapons.'[647] The interpretation of this statement

[643] Justin McClelland, 'The Review of Weapons in Accordance with Article 36 of Additional Protocol I' (2003) 85 *International Review of the Red Cross* 412.
[644] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts art. 36, June 8, 1977, 1125 U.N.T.S. 3 reprinted in Dietrich Schindler & Jiri Toman (eds), *The Laws of Armed Conflicts: A Collection of Conventions, Resolutions, and Other Documents* (Brill – Nijhoff, 4th edition, 2004) 730.
[645] Geoffrey Best, *War and Law Since 1945* (Clarendon Press, 1994) 306.
[646] Jean de Preux, 'Article 36-New Weapons' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 423.
[647] Report to Third Committee on the Work of the Working Group Committee III CDDH/III/293 in Howard Levie, *Protection of War Victims: Protocol I to the 1949 Geneva Conventions* (Oceana Publications, 1980) 289.

indicates that Article 36 does not oblige states to review existing weapons. However, weapons review mechanisms cover the reassessment of existing weapons. For instance, if a state becomes a party to a treaty that prohibits the use of a particular weapon (such as the Ottawa Convention, which forbids anti-personnel mines) a state must reassess existing weapons. On the one hand, the reviewing process is not a one-time event, so when a weapon is dramatically modified and/or used in a new way, reassessment will be required. On the other hand, when a particular state determines that a particular weapon is either legal or illegal, this ruling does not necessarily apply to other states, which must conduct their own reviews. Similarly, when a state completes the review process when acquiring a weapon or munition, other states must still complete their own reviews when acquiring the same weapon or munition.

Some states review their weapons regularly, [648] but is it possible to review the legality of weapons which are not yet developed? Legal reviews can take place at different stages of a weapon's development, so there is no reason not to review a weapon as it is being developed. Therefore, states should assess the legality of a weapon before a new stage in order to prevent international criticism. Finally, states that manufacture weapons are not solely responsible to observe Article 36. [649] It is currently the only mechanism that Article 36 reviews which prevents an arms race; therefore, a wide range of applications must be made to existing and future weapons. [650]

State Weapon Review Procedures – Article 36

Because many states do not perform their legal reviews of new weapons obligation, and those that do keep the specifics out of the public domain, determining the present status of such reviews is a challenging task. Furthermore, states with publicly-available reviews vary greatly in terms of review practices.

[648] 'The United Kingdom puts the legality of its weapons and methods of warfare under regular consideration.' Joshua Hughes, 'The Law of Armed Conflict Issues Created by Programming Automatic Target Recognition Systems Using Deep Learning Methods' in Terry Gill, Robin Geiss, Heike Krieger, Christophe Paulussen (eds) *Yearbook of International Humanitarian Law* (The Hague: T.M.C. Asser Press, 2019) 123.
[649] Avril McDonald, 'The International Legality of Depleted Uranium Weapons' Presentation at the Symposium on the Health Impact of Depleted Uranium Munitions' 26-27 (June 14, 2003), http://www.nuclearpolicy.org/files/nuclear/mcdonald-jun-14 03.pdf
[650] Jean de Preux, 'Article 36-New Weapons' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 427.

Based on the information available, it appears that many states are failing to comply with the requirements of Article 36. Demand for the time it takes to design and use weapons to be reduced began to rise rapidly during the Cold War[651], with demand continuing despite the conflict's end. Weapon use is limited by legal reviews, providing some explanation as to why many states seem to have avoided compliance with Article 36. Since the First Additional Protocol was first adopted 41years ago, only the US, Canada, the UK, Australia, the Netherlands, Sweden, Norway, Germany, Denmark, and Belgium have implemented official review procedures, with the remaining 164 out of 174 states failing to put such procedures in place.[652] Additionally, given that the US already had official review procedures in place prior to the creation of Article 36, and given that the US is not party to the First Additional Protocol, the review procedures do not necessarily demonstrate that compliance with Article 36 is the motivation behind such procedures. It is possible that unofficial review procedures still exist, but because no information about these procedures is available in the public domain, this cannot be confirmed for certain.

The intentions of various states regarding their duty to comply with the requirements of Article 36 were publicised through statements made during the drafting stage, at which time the UK, Canada, Germany, and the Netherlands stated their intention to put weapon deployment review procedures in place, whilst the US and Sweden declared that they already implemented weapon deployment review procedures. Review practice in Switzerland and the Russia has taken shape since the introduction of Article 36, although neither state confirmed that official review procedures would be implemented, acknowledging only states' responsibility to evaluate the lawful use of national weapons.[653] No information could be accessed regarding review procedure in Germany, Denmark, or Canada despite these states claiming to have official review procedures in place[654]. Therefore, the following sections discuss the review procedures of Australia, New Zealand, the Netherlands, Norway, Sweden, Switzerland, United Kingdom and the US based on the limited information available.

---

[651]Victor Larionov, 'Russian Military Doctrine/Strategy, Future Security Threats and Warfare' in Sharyl Cross et al. (eds), *Global Security Beyond the Millennium: American and Russian Perspectives* (Palgrave Macmillan, 1999) 238.
[652] Donna Verchio, 'Just Say No! The SIrUS Project: Well-Intentioned, but Unnecessary and Superfluous' (2001) 51 *Air Force Law Review* 183, 213.
[653]Damian Copeland, 'Legal Review of New Technology Weapons' in Hitoshi Nasu and Robert McLaughlin (eds), *New Technologies and the Law of Armed Conflict* (Asser Press, 2014) 43.
[654]Damian Copeland, 'Legal Review of New Technology Weapons' in Hitoshi Nasu and Robert McLaughlin (eds), *New Technologies and the Law of Armed Conflict* (Asser Press, 2014) 43.

Australia

The legal use of weapons is governed by the Director-General of the Defence Legal Service at the Ministry of Defence in Australia.[655] When reviewing the use of weapons, the Director-General must take into account medical, military and legal considerations,[656] with recommendations that information from numerous experts should be obtained for the purpose of assessing the impacts of weapon use.[657] The ICJ criteria for weapon legality requires to determine whether there is a law or rule preventing the weapon from being used, and whether there is a general legal principle that prevents the use of the weapon.[658] The question then becomes a decision of ethics versus national security, with the Director-General determining whether it is necessary for the weapon to be used[659] and should engage in a balancing test between military necessity and unnecessary suffering based on the target region of use, the speed with which the weapon causes damage, versus environmental considerations, consideration of human suffering, superfluous injury and is indiscriminate.[660] The weapon will either be restricted or prohibited if it does not pass these requirements, or if it is considered unlawful in the international context.[661]

New Zealand

The review process in New Zealand is known as Article 36, based on the Geneva Conventions Act (1958) and initiated by the Chief of Defence Force issuing Defence Force Orders in accordance with the 1990 Defence Act (section 27).[662]

'Weapons' and 'munitions' are defined in the Manual of Armed Forces Law as being anything designed or modified in order to inflict damage on opposition forces; this includes arms, firearms,

[655] Legal Review of New Weapons, Australian Department of Defence Instruction (General) OPS 44-1, 2 June 2005.
[656] Legal Review of New Weapons, Australian Department of Defence Instruction (General) OPS 44-1, 2 June 2005.
[657] Legal Review of New Weapons, Australian Department of Defence Instruction (General) OPS 44-1, 2 June 2005.
[658] The International Court of Justice *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*, 8 July 1996, paragraph 87.
[659] Legal Review of New Weapons, Australian Department of Defence Instruction (General) OPS 44-1, 2 June 2005.
[660] Legal Review of New Weapons, Australian Department of Defence Instruction (General) OPS 44-1, 2 June 2005.
[661] Legal Review of New Weapons, Australian Department of Defence Instruction (General) OPS 44-1, 2 June 2005.
[662] The Manual of Armed Forces Law (Second Edition) Volume 4 '*Law of Armed Conflict*' Defence Force Order Chapter 7, Section 4 <http://www.nzdf.mil.nz/downloads/pdf/public-docs/> accessed on 29 March 2018.

weapons systems, explosives, missiles and bombs. Weaponry that is not currently used or in development comes under this definition.[663]

The prime driver for Article 36 reviews is International Humanitarian Law. The reviews also consider any other relevant treaties to which New Zealand is signatory; for example, the Convention on Cluster Munitions (2008)[664]. There is no specific consideration of the Martens Clause, but the review does consider the way in which the weapon may be used.[665] The ways in which the review is conducted may vary depending on the requirements of the New Zealand Defence Force, but it begins as soon as the Force begins to consider new weaponry, even if such weaponry is just being trialled. If operational requirements dictate, reviews may be fast-tracked.[666]

The chief witnesses summoned will include specialists on a particular munition or weaponry being examined from the Armed Forces, civilians with appropriate expertise, legal experts from the New Zealand Defence Force, and any relevant contributors from other branches of government; for example, the Crown Law Office. Arms manufacturers may also be asked to contribute.[667]

All pertinent treaties, as well as applicable international law, will be considered by the review; in addition, the ways in which the weaponry is likely to be deployed are examined. Part of the process involves examining the ways in which the amount of explosives left behind after a conflict can be minimised. The ways in which laws of warfare may develop in future also come under consideration, as too are the methods that other states have used to deploy weaponry or munitions and the opinion of those states on the legality of these weapons. The aim of the review is to conclude if the weaponry or munitions in question may be legally introduced. The review may create conditions regarding the use of the weaponry. The decision that is made during the review is final, and any weaponry or munitions that do not satisfy the requirements of the Director of

[663] The Manual of Armed Forces Law (Second Edition) Volume 4 '*Law of Armed Conflict*' Defence Force Order Chapter 7, Section 4 <http://www.nzdf.mil.nz/downloads/pdf/public-docs/> accessed on 29 March 2018.
[664] Convention on Cluster Munitions, opened for signature 3 Dec. 2008, entered into force 1 Aug. 2010.
[665] The Manual of Armed Forces Law (Second Edition) Volume 4 '*Law of Armed Conflict*' Defence Force Order Chapter 7, Section 4 <http://www.nzdf.mil.nz/downloads/pdf/public-docs/> accessed on 29 March 2018.
[666] The Manual of Armed Forces Law (Second Edition) Volume 4 '*Law of Armed Conflict*' Defence Force Order Chapter 7, Section 4 <http://www.nzdf.mil.nz/downloads/pdf/public-docs/> accessed on 29 March 2018.
[667] The Manual of Armed Forces Law (Second Edition) Volume 4 '*Law of Armed Conflict*' Defence Force Order Chapter 7, Section 4 <http://www.nzdf.mil.nz/downloads/pdf/public-docs/> accessed on 29 March 2018.

Defence Legal Services' review may not be put into development, purchased or used in service. There is no mechanism for any application for review or appeal.[668] The New Zealand Defence Force keeps its own records of the reviews that have been undertaken, as per its statutory obligations (although there has only been one review in the last ten years). These records may be accessed by government and military entities, and the public may also be able to access the information if permitted by the Official Information Act (1982).[669]

The Netherlands

The legality of weapons in the Netherlands is determined by the Advisory Commission on International Law and Conventional Weapons Use, established on the 5th of May 1978, based on a decree by the Minister of Defence. The Advisory Commission is comprised of numerous members of the Dutch Ministry of Defence, including the Director of Legal Affairs, the Director of Military Medical Services, the Director of General Policy Affairs, the Director-General of Materiel, the Dutch Chief of Staff, and chiefs of the armed services.[670] Furthermore, three representatives from the Ministry of Foreign Affairs can also participate in the Commission's activities on the invitation of the Minister of Foreign Affairs.[671] Whilst no formal legal authority is held by the Minister of Defence's decree, the Advisory Commission provides counsel to the Minister as to whether a weapon complies with international law in terms of what can be acquired, held or deployed by the Dutch military.[672] The Advisory Commission is presently under review, although no further information is available with regards to the specific weapon review procedures used by the Commission at this time.

---

[668] The Manual of Armed Forces Law (Second Edition) Volume 4 '*Law of Armed Conflict*' Defence Force Order Chapter 7, Section 4 <http://www.nzdf.mil.nz/downloads/pdf/public-docs/> accessed on 29 March 2018.
[669] The Manual of Armed Forces Law (Second Edition) Volume 4 '*Law of Armed Conflict*' Defence Force Order Chapter 7, Section 4 <http://www.nzdf.mil.nz/downloads/pdf/public-docs/> accessed on 29 March 2018.
[670]For a detailed summary of the various approaches of States; Isabella Daoust, Robin Coupland and Rikke Ishoey, 'New Wars, New Weapons? The Obligation of States to Assess the Legality of Means and Methods of Warfare' (2002) 84 *International Review of the Red Cross* 354. The Netherlands: *Beschikking van de Minister van Defensie* (Directive of the Minister of Defence) nr. 458.614/A, 5 May 1978, establishing the *Adviescommissie Internationaal Recht en Conventioneel Wapengebruik* (Committee for International Law and the Use of Conventional Weapons).
[671]The Netherlands: *Beschikking van de Minister van Defensie* (Directive of the Minister of Defence) nr. 458.614/A, 5 May 1978, establishing the *Adviescommissie Internationaal Recht en Conventioneel Wapengebruik* (Committee for International Law and the Use of Conventional Weapons).
[672]The Netherlands: *Beschikking van de Minister van Defensie* (Directive of the Minister of Defence) nr. 458.614/A, 5 May 1978, establishing the *Adviescommissie Internationaal Recht en Conventioneel Wapengebruik* (Committee for International Law and the Use of Conventional Weapons).

Norway

The Norwegian review committee is chaired by the Legal Services Office of the Defence Command, and began operations in 1999 after being established five years prior. The committee is comprised of officials from the Norwegian Defence Research Establishment, the Defence Staff College, the Logistics Resources Management Division, and the Army Material Command; with no representative of the Department of Defence.[673] The committee meets four times a year, as meeting more regularly would require a change in its structure and size. Based on the feedback of experts from numerous official bodies, weapons are reviewed by the committee during the early stages of developing or acquiring weapons.[674] However, if amendments are made to the legal requirements of Norwegian weapon use, the committee is also responsible for reviewing weapons that are already owned or being deployed.[675] Furthermore, whilst the committee has no authority to prevent weapon production, is does set the legal review criteria for the development of new weapons.[676]

Sweden

The Swedish weapon review committee, The Delegation for International Humanitarian Law Monitoring of Arms Projects, is governed primarily by the Swedish Ministry of Defence, and is comprised of numerous experts from the technical, medical, military, and legal fields.[677] In 1974, Sweden challenged the legality of weapons deployed in Vietnam, leading the state to become a pioneer in the arena of official weapon review. Meetings are held three or four times annually, or more frequently if required.[678] The committee reviews both weapons of its own selection as well

[673] Norway: *Direktiv om folkerettslig vurdering av vapen, krigforingsmetoder og krigforingsvirkemidler*, (Directive on the Legal Review on Weapons, Methods and Means of Warfare), Ministry of Defence, 18 June 2013.
[674] Norway: *Direktiv om folkerettslig vurdering av vapen, krigforingsmetoder og krigforingsvirkemidler*, (Directive on the Legal Review on Weapons, Methods and Means of Warfare), Ministry of Defence, 18 June 2013.
[675] Norway: *Direktiv om folkerettslig vurdering av vapen, krigforingsmetoder og krigforingsvirkemidler*, (Directive on the Legal Review on Weapons, Methods and Means of Warfare), Ministry of Defence, 18 June 2013.
[676]Norway: *Direktiv om folkerettslig vurdering av vapen, krigforingsmetoder og krigforingsvirkemidler*, (Directive on the Legal Review on Weapons, Methods and Means of Warfare), Ministry of Defence, 18 June 2013.
[677]Vincent Boulanin and Maaike Verbruggen, 'Compendium on Article 36 reviews' (2017) SIPRI Background Paper Stockholm International Peace Research Institute <https://www.sipri.org/publications/2017/sipri-background-papers/sipri-compendium-article-36-reviews> (accessed on 29 March 2018) citing Sweden: *Förordning om folkrättslig granskning av vapenproject* (Ordinance on international law review of arms projects), Swedish Code of Statutes, SFS2007:936.
[678]Sweden: *Förordning om folkrättslig granskning av vapenproject* (Ordinance on international law review of arms projects), Swedish Code of Statutes, SFS 2007:936.

as weapons in development based on reports from the Swedish Armed Forces.[679] The Swedish government is then informed by the committee about any legality issues, with the government having the authority to make changes to weapons in order to meet international law requirements, or to reject the development or use of a weapon altogether.[680]

Switzerland

Swiss law has required legal reviews of weaponry from 2007 onwards. The type of weaponry that should be reviewed is not formally defined, but there is a general principle that all new weaponry should be examined. Additionally, any weaponry that is adapted in a way that changes its performance or the ways in which it can be used should also be reviewed. New methods of warfare are also legally reviewed.[681]

These reviews take into account both the relevant sections of international law and the treaties to which Switzerland is a signatory. If a weapon has the potential to be used in law enforcement, international human rights law may also be considered. These legal reviews run concurrent with the length of the procurement mechanisms, starting with draft specifications when projects are being planned. Weaponry can then be legally reviewed again once a particular model or manufacturer has been chosen; the final procurement decision is subject to definitive agreements that the weaponry complies with all relevant international legislation.[682] The Law of Armed Conflict Section may undertake consultations with specialists in all relevant areas during the review process.[683]

---

[679]Sweden: *Förordning om folkrättslig granskning av vapenproject* (Ordinance on international law review of arms projects), Swedish Code of Statutes, SFS 2007:936.
[680]Sweden: *Förordning om folkrättslig granskning av vapenproject* (Ordinance on international law review of arms projects), Swedish Code of Statutes, SFS 2007:936.
[681] Ordonnance du Département fédéral de la défense, de la protection de la population et des sports (DDPS) sur le matériel de l'armée (OMat) [Ordinance of the Swiss Federal Department of Defence, Civil Protection and Sport (DDPS) on the equipment of the armed forces], Law no. 514.20, 6 Dec. 2007; and Weisungen über das Armee material (WAMAT) [Directive on the equipment of the armed forces], 4 Mar. 2009, <https://www.vtg.admin.ch/internet/vtg/de/home/themen/zsham>.
[682] Ordonnance du Département fédéral de la défense, de la protection de la population et des sports (DDPS) sur le matériel de l'armée (OMat) [Ordinance of the Swiss Federal Department of Defence, Civil Protection and Sport (DDPS) on the equipment of the armed forces], Law no. 514.20, 6 Dec. 2007; and Weisungen über das Armee material (WAMAT) [Directive on the equipment of the armed forces], 4 Mar. 2009, <https://www.vtg.admin.ch/internet/vtg/de/home/themen/zsham>.
[683] Ordonnance du Département fédéral de la défense, de la protection de la population et des sports (DDPS) sur le matériel de l'armée (OMat) [Ordinance of the Swiss Federal Department of Defence, Civil Protection and Sport (DDPS) on the equipment of the armed forces], Law no. 514.20, 6 Dec. 2007; and Weisungen über das Armee material

United Kingdom

In 1998, the Additional Protocol 1 from the Geneva Conventions (1949) was ratified by the UK and, simultaneously, the country introduced a system for formal review. Before this date, reviews had been undertaken by the MoD (Ministry of Defence), but they are now undertaken by the Development, Concepts and Doctrine Centre (DCDC), a satellite entity that utilises military lawyers from all branches of the armed services to undertake reviews on the MoD's behalf.[684]

Once the DCDC has undertaken a review, it usually offers a formal opinion in writing. This is signed by the military lawyers involved; however, there is a collaborative element in the process: All those who have contributed to it, particularly any experts who may have given opinions, have to offer confirmation before providing their signature to confirm that all the facts contained in the advice are accurate. The advice is then subject to a peer review by another of the DCDC's lawyers.[685] All new weaponry, and other ways and means of conducting war, is legally reviewed by the UK. The term weapon is understood to refer to the widest possible field of meanings. As well as reviewing all new weaponry, weaponry that has been adapted for another purpose will also be reviewed. The review examines the design of the weaponry and the ways in which it is intended to be used.[686]

The amount of time the review takes entirely depends on the subject at hand. When a quick decision is required, for example when weaponry needs to be adapted to fit current operations, the review may be fast-tracked; alternatively, the review may last as long as it takes to develop the weaponry.[687]

(WAMAT) [Directive on the equipment of the armed forces], 4 Mar. 2009, <https://www.vtg.admin.ch/internet/vtg/de/home/themen/zsham>

[684] UK Ministry of Defence Development Concepts and Doctrine Centre, UK Weapon Reviews (2016) <https://www.gov.uk/government/publications/uk-weapon-reviews>.

[685] UK Ministry of Defence Development Concepts and Doctrine Centre, UK Weapon Reviews (2016) https://www.gov.uk/government/publications/uk-weapon-reviews.

[686] UK Ministry of Defence Development Concepts and Doctrine Centre, UK Weapon Reviews (2016) <https://www.gov.uk/government/publications/uk-weapon-reviews>.

[687] UK Ministry of Defence Development Concepts and Doctrine Centre, UK Weapon Reviews (2016) <https://www.gov.uk/government/publications/uk-weapon-reviews>.

During the review, all relevant documents from the manufacturer will be considered, as well as evidence from the services. The documentation will be different in each case and may include evidence gained from many consultations with the appropriate experts. Further independent tests may be undertaken by the MoD to confirm that the information that the manufacturer provided about the weapon is correct.[688]

Those consulted during the review will include the individuals who are concerned with testing and procuring equipment for the services, expert medical witnesses, government scientists, experts from all branches of the services, authorities on the environment, and the businesses and engineers responsible for designing and building the equipment in question.[689]

United States

Weapon review in the US is carried about by individual officials, rather than review committees, who are responsible for ensuring that weapons are 'consistent with all applicable domestic law and treaties and international agreements, … customary international law, and the law of armed conflict.'[690] Following the Vietnam War and in an attempt to achieve national implementation of IHL, the US appears to have been carrying out official weapon review since 1974. Whilst the appointment of individual weapon review officials allows for meetings to be held when needed, whilst also ensuring less variance between reviews, the US Air Force, Navy, and Army's use of in-house review procedures means that variance still exists across different departments of the military.[691] One official is appointed to review weapons that are being developed by multiple departments, however, which does help in this respect. Nonetheless, it is impressive that the US

[688] UK Ministry of Defence Development Concepts and Doctrine Centre, UK Weapon Reviews (2016) <https://www.gov.uk/government/publications/uk-weapon-reviews>.
[689] UK Ministry of Defence Development Concepts and Doctrine Centre, UK Weapon Reviews (2016) <https://www.gov.uk/government/publications/uk-weapon-reviews>.
[690] U.S. Department of Defense Directive (DoDD) 5000.01 The Defense Acquisition System T El. 15 (May 12, 2003) available at <http://www.dtic.mil/whs/directives/corres/pdf2/d50001p.pdf> (accessed 2 January 2018) ('An attorney authorized to conduct such legal reviews in the Department shall conduct the legal review of the intended acquisition of weapons or weapons systems.').
[691] The United States: Review of Legality of Weapons under International Law, US Department of Defense Instruction 5500.15, 16 October 1974; Weapons Review, US Department of Air Force Instruction 51-402, 13 May 1994; Legal Services: Review of Legality of Weapons under International Law, US Department of Army Regulation 27-53, 1 January 1979; Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System, US Department of Navy, Secretary of the Navy Instruction 5000.2C, 19 November 2004; Policy for Non-Lethal Weapons, US Department of Defense Directive 3000.3, 9 July 1996; The Defense Acquisition System, US Department of Defense Directive 5000.1, 12 May 2003.

implements official weapon review procedures as standard despite it is not a party to the First Additional Protocol. Furthermore, the US also reviews existing weapons if significant changes have been made to these weapons, which is an approach that other states may adopt from.

Similarities Between State Review Procedures

As evident from the previous sections, there are a number of similarities in the review procedures adopted by the eight aforementioned states despite the various differences between them. Firstly, formal weapon reviews are largely carried out by the armed forces and/or Ministry of Defence, with input from environmental, technical, medical, and other relevant experts and officials. This is a key strength in the approach of these states, as highlighted in the January 2001 ICRC meeting.[692] The second similarity between the eight states' approaches to weapon review is the emphasis placed on the timely evaluation of weapon legality. Here, it is evident that the eight states review weapons before they are deployed, with some reviews performed during the development stage. Not only is this an effective approach from an ethical standpoint, it also reduces the risk of incurring heavy manufacturing costs for weapons that could be prohibited upon review. Thirdly, as seen in the case of Sweden, where the act of sharing information on weapons is permissible under the Swedish Secrecy Act, and in the case of the US, where weapon information can be shared under the Freedom of Information Act, numerous states take a position in which national security is protected whilst transparency is maintained.

Suggested State Review Practices

The structure of reviews under Article 36 are unsupported by official guidelines[693], with states resisting recommendations that an impartial and standardised system be put into place.[694]

The ICJ Advisory Opinion in the *Nuclear Weapons Case* provides official guidelines for weapon review procedure, with these guidelines appearing to refer to both nuclear and other types of weapons. The guidelines suggest that if neither customary law nor treaty specifically prohibits a

[692] Summary Report by the ICRC, Expert Meeting on Legal Reviews of Weapons and the SIrUS Project, Jongny sur Vevey, Switzerland (29-31 January 2001).
[693] William Boothby, *Weapons and the Law of Armed Conflict* (Oxford University Press, 2009) 341.
[694] Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (CUP, 2004) 80.

given weapon, the party responsible for the review must assess whether the weapon should be prohibited based on a more general overview of customary law or treaty law.[695]

According to Daoust, Copeland and Ishoey, weapon reviews should be carried out with recognition that the provision 'implies, as a first step in the review, an examination of the specific prohibitions found under international law to which the reviewing State is a party and which bans or restricts the use of a weapon or method of warfare'.[696] It is also obligatory for states to take customary international law into account, particularly in terms of the principle of distinction, prohibition of unnecessary suffering and indiscriminate attack[697], as well as the prohibition on causing significant, long-term and large-scale environmental damage stated under Article 35(3).[698] The researchers further add that 'the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience' (the Martens Clause)[699] should be considered as part of weapon review. *The Nuclear Weapons Advisory Opinion* asserted that the Martens Clause has 'continuing existence and applicability' in the review of new weapons, and that it has also 'proved to be an effective means of addressing the rapid evolution of military technology'.[700] The researchers summarise that weapon reviews should consider the potential consequences of the widespread use of the weapon, the way in which the weapon will be used in different situations and settings, and whether the same objectives could be achieved with alternative weapons or approaches.

Additional recommendations were made at the January 2001 ICRC meeting, which was held with the purpose of addressing review procedures based on the ICRC's recent work on superfluous injury and unnecessary suffering caused through the use of weapons. Here, it is suggested that state weapon reviews must be extensive, and that they must be informed by experts from various

[695] Bruce Oswald, 'The Australian Defence Force Approach to the Legal Review of Weapons' *Australian and New Zealand Society of International Law 2001 Proceedings Papers*, 63. Note the assessment in the *Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)* [1996] I.C.J. Rep [53]-[63].
[696] Isabella Daoust, Robin Coupland and Rikke Ishoey, 'New Wars, New Weapons? The Obligation of States to Assess the Legality of Means and Methods of Warfare' (2002) 84 *International Review of the Red Cross* 349.
[697] *Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)* [1996] I.C.J. Rep [78].
[698] Isabella Daoust, Robin Coupland and Rikke Ishoey, 'New Wars, New Weapons? The Obligation of States to Assess the Legality of Means and Methods of Warfare' (2002) 84 *International Review of the Red Cross* 350.
[699] Isabella Daoust, Robin Coupland and Rikke Ishoey, 'New Wars, New Weapons? The Obligation of States to Assess the Legality of Means and Methods of Warfare' (2002) 84 *International Review of the Red Cross* 351.
[700] *Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)* [1996] I.C.J. Rep [78], [87]

fields, particularly in terms of the review of weapons that cause injuries beyond burns, projectile force or explosion, as well as when weapons cause damage that is not well known or experienced.[701]

Conclusion

As highlighted throughout this chapter, the legality of autonomous weapons is a difficult feat to achieve, from a technical level. Whilst further work is needed in relation to the considerations outlined in the above sections, a number of recommendations for best practice in state weapon review procedures can be made.

Firstly, it is recommended that reviews are performed either during the conception of a weapon or as early as it is feasible to do so. It would be greatly beneficial if weapon review was to become a mandatory part of weapon acquirement, with written documentation stored so as to ensure that guidelines are followed through to the adoption and deployment of the weapons in question.

The second recommendation for best practice in state weapon review is the inclusion of technical, medical, legal, and other experts in the review process. Technical and operational expert input is particularly valuable given the insight that can be gained in terms of the potential damage that can be caused by a weapon and whether this complies with the given requirements.

Thirdly, it is recommended that technological developments would be better understood by military lawyers enlisted for the purpose of weapon review if they were to undergo a degree of technical training. Similarly, weapon designers, system developers, and engineers would benefit from understanding relevant international laws in order to ensure that the weapons they design comply with legal requirements.

Additionally, it is recommended that state reviews of weapon legality factor in empirical findings from governments, militaries and weapon manufacturers whilst also performing their own investigations, in collaboration with relevant parties, into weapon performance and dangers. The development and future use of weapon reviews can be better understood through greater

[701] Summary Report of the ICRC Expert Meeting, Switzerland (29-31 January 2001).

partnership and communication between the government, the military, system developers, lawyers, and technical experts. The potential for such an approach to increase collaboration with the military may be explored, given the costs involved in carrying out such tests, as this would help to determine the best procedures and approaches for testing weapon features.

Finally, restrictions on the use of autonomous weapons should be determined based on the evaluation of their operational and technical performance, with a focus on factors such as the target type and deployment attributions. In other words, restrictions could be based on whether weapon is designed for personnel or materiel targets, the duration for which the weapon will deployed, and the environment in which the weapon will be deployed.

Chapter 6 - The Responsibility of States for Internationally Wrongful Acts

Introduction

States are responsible for the conduct of their organs, and those acting under the direction, instigation, or control of these organs.[702] Obviously, the AWS itself is not an "organ" of a State. There is first the question of state responsibility where the State uses an autonomous weapon, and a state agent launches it. Second, where the State has contracted with the private military company (PMC), is there a basis for holding the State responsible for the acts of the PMC, even though they are not State agents in the way in which members of the armed forces are? Third, this chapter includes reference to the possibility of proceedings based on the violation of IHL. This chapter only focuses on the legal liability of the state.

State Responsibility

Article 2 of the Draft Articles for state responsibility (ASR) provides a point of departure for any application of the law of state responsibility:[703]

'There is an internationally wrongful act of a state when conduct consisting of an action or omission: (a) is attributable to the state under international law; and (b) constitutes a breach of an international obligation of the state.'

Relevant wrongful acts concern weapon use that breaches a state's international humanitarian law (IHL) obligations. Such breaches are caused by events that could relate equally to the use of either autonomous or manually-operated weapons. For instance, a state may cause civilian deaths if it identifies a target or plans an attack without taking the appropriate precautions. Because autonomy does not relate to a weapon type but, rather, to the manner in which it is controlled, violent acts such as the discharging of a weapon are no different for autonomous weapons than they are for manual systems. For an AWS, the system discharging its weapon would constitute the immediate

[702] Thilo Marauhn, '*Responsibility and Accountability*' Presentation at United Nations Office Geneva, 13-16 May 2014, 6

[703] Articles on Responsibility of States for Internationally Wrongful Acts, Report of the International Law Commission, 53rd Session, UN Doc. A/56/10 (2001), 43–59 (noted in GA Res. 56/83, 12 December 2001, UN Doc. A/RES/56/83 (2001)).

cause of a violent act, in the same way that a soldier pulling the trigger on their rifle would be the immediate cause of another.

When evaluating state responsibility for the harm caused to objects or individuals, the conduct of interest is that which causes the weapon to be discharged. When AWS are used in an attack, it is particularly difficult to attribute responsibility to the state. Any such difficulty is caused by an accountability gap associated with their usage. Indeed, many AWS opponents often cite this gap when campaigning for their prohibition or restriction.[704]

In order to attribute responsibility for AWS conduct to the state that deploys the system, it is first necessary to recognise states as being responsible, during the course of an armed conflict, for the associated actions of the service personnel within their military forces. Therefore, during the course of an armed conflict, should a member of a state's military forces intentionally kill a civilian using a manual weapon or rifle and, as such, break the law, responsibility for this violent act would be easily attributed to the state due to state agent status of a soldier.

What is important to consider, however, is whether this situation may change if the weapon discharged by the individual had a degree of autonomy and, indeed, how it would change. Should a state organ, such as a military service person or any other state-employed individual, use an AWS in such a way that it inflicts harm and violates relevant law in doing so, the state would be accountable for these actions in the same way that it would for illegal use of manual weaponry. In cases where no state organ has performed any such action, the state will not be accountable. According to existing IHL, states are responsible for the decisions made by its militaries when selecting an AWS for an attack and when activating that AWS at a specific place and time. If the harm that results from an AWS attack is not attributable to the state, the chain of responsibility must be disturbed by some feature of the AWS. While it is a minority view, some researchers

[704] Christof Heyns, 'Autonomous Weapons Systems: Living a Dignified Life and Dying a Dignified Death' in Nehal Bhuta et al. (eds), *Autonomous Weapons Systems: Law, Ethics, Policy* (Cambridge University Press, 2016) 20; Alex Leveringhaus, *Ethics and Autonomous Weapons* (Palgrave Macmillan, 2016) 114; William Fleischman, 'Just Say No! to Lethal Autonomous Robotic Weapons' (2015) 13 *Journal of Information, Communication and Ethics in Society* 313.

believe that highly autonomous AWS could make it difficult to determine state responsibility for their actions.[705]

AWS and the Law of State Responsibility

According to Crawford, the law of state responsibility is a 'cardinal institution of international law.'[706] Communicated by the International Law Commission and adopted in 2001, the Draft Articles on the Responsibility of States for Internationally Wrongful Acts[707] provide a key reference for the law of state responsibility.[708] The articles do not, however, explain the extent of international obligations; they simply detail the requisite conditions for, and resulting consequences of, breaches to these obligations. The Draft Articles are not legally binding[709] but they are widely considered, however, as a codification of customary law.[710] Since their introduction, the Draft Articles have been referenced in a number of United Nations General Assembly resolutions.[711] Further, the ICJ applied an early draft text in the *Gabčíkovo-Nagyamaros Project (Hungary/Slovakia)* case.[712]

[705] Daniele Amoroso and Benedetta Giordano, 'Who Is to Blame for Autonomous Weapons Systems' Misdoings?' in Elena Carpanelli and Nicole Lazzerini (eds), *Use and Misuse of New Technologies* (Springer, 2019) 225; Daniel Hammond, 'Autonomous Weapons and the Problem of State Accountability' (2015) 15 *Chicago Journal of International Law* 687.

[706] James Crawford, 'State Responsibility' in Max Planck Encyclopedia of Public International Law (2006) [1] <http://opil.ouplaw.com/home/EPIL>.

[707] ILC Report 43 ('Draft Articles').

[708] Report of the International Law Commission, UN GAOR, 56th sess, Supp No 10, UN Doc A/56/10 (2001) ('ILC Report'). Frits Kalshoven, 'State Responsibility for Warlike Acts of the Armed Forces' (1991) 40 *International and Comparative Law Quarterly* 827; Dieter Fleck, 'Individual and State Responsibility for Violations of the Ius in Bello: An Imperfect Balance' in Wolff Heintschel von Heinegg and Volker Epping (eds), *International Humanitarian Law Facing New Challenges* (Springer, 2007) 171; Markus Rau, 'State Liability for Violations of International Humanitarian Law — The Distomo Case before the German Federal Constitutional Court' (2006) 7 *German Law Journal* 701.

[709] See, eg, *Prosecutor v Nikolić* (Decision on Defence Motion Challenging the Exercise of Jurisdiction by the Tribunal) (International Criminal Tribunal for the Former Yugoslavia, Trial Chamber II, Case No IT–94–2–PT, 9 October 2002) [60].

[710] See, eg, *Noble Ventures Inc v Romania* (Award) (ICSID Arbitral Tribunal, Case No ARB/01/11, 12 October 2005) [69].

[711] Responsibility of States for Internationally Wrongful Acts, UN GAOR, 6th Comm, 56th sess, 85th, Agenda Item 162, UN Doc A/RES/56/83 (12 December 2001); Responsibility of States for Internationally Wrongful Acts, UN GAOR, 6th Comm, 59th sess, 65th, Agenda Item 139, UN Doc A/RES/59/35 (2 December 2004); Responsibility of States for Internationally Wrongful Acts, UN GAOR, 6th Comm, 62nd sess, 62nd, Agenda Item 78, UN Doc A/RES/62/61 of 6 December 2007; Responsibility of States for Internationally Wrongful Acts, UN GAOR, 6th Comm, 65th sess, 57th, Agenda Item 75, UN Doc A/RES/65/19 (6 December 2010).

[712] *Gabčíkovo-Nagyamaros Project (Hungary v Slovakia)* (Judgment), [1997] ICJ Rep 7, 35 [47].

States are considered responsible for any 'internationally wrongful act' they perform that, as an act or omission, breaches one of their international obligations and is attributable to them.[713] In legal terms, state obligations comprise any customary or treaty obligations, whether such obligations refer to a state's behaviour towards the international community as a whole, towards a non-state body, or towards another state. Typically, when acts and omissions are considered in terms of state obligations, this consideration is not influenced by the resulting harm or by the intentions of the responsible entity. This only differs if the primary rule applied specifies such conditions.[714]

The discussion becomes more complex when it examines which specific acts and omissions are attributable to the state. Because states cannot act alone, any act 'of the state' is an act conducted by individuals or groups whose behaviour is, in the given conditions, a state responsibility. Without a clear list defining the individuals and groups whose behaviour is attributable to the state, 'the general rule is that the only conduct attributed to the state at the international level is that of its organs of government, or of others who have acted under the direction, instigation or control of those organs, i.e. as agents of the state.'[715] When identifying responsibility, '[a]n organ includes any person or entity which has that status in accordance with the internal law of the state',[716] even if the conduct of such individuals or entities exceeds their authority or contravenes their instructions.[717] Generally, states are not accountable for the behaviour of private parties except human rights obligations; however, 'a state may be responsible for the effects of the conduct of private parties, if it failed to take necessary measures to prevent those effects.'[718]

[713] Draft Articles arts 1, 2; also ILC Report 68-9 [1]-[2].
[714] For example, the Convention on the Prevention and Punishment of the Crime of Genocide defines genocide as '… any of the following acts committed with intent to destroy, in whole or in part, a national, ethnical, racial or religious group, …'.
[715] Materials on the Responsibility of States for Internationally Wrongful Acts, United Nations Legislative Series Book 25, UN Doc ST/LEG/SER.B/25, (2012) 27 [2] ('Materials on the Responsibility of States for Internationally Wrongful Acts').
[716] Draft Articles art 4; see also art 5 for entities exercising governmental authority.
[717] Draft Articles art 7.
[718] Materials on the Responsibility of States for Internationally Wrongful Acts, 28 [4].

In both peacetime and wartime, IHL imposes a number of positive and negative obligations on states, by way of their organs.[719] For the purpose of this discussion, the relevant obligations are those which apply to military personnel when planning and executing attacks. In particular, they concern the obligation to take precautions when verifying that targets are legitimate and that the selected means and methods of warfare are appropriate.

Performing as a set of default rules, the Draft Articles can be superseded by certain secondary rules, relevant to specialist legal areas. Entitled '*lex specialis'*, Article 55 states that the Draft Articles 'do not apply where and to the extent that the conditions for the existence of an internationally wrongful act or the content or implementation of the international responsibility of a state are governed by special rules of international law.'

The Draft Articles are universally accepted as a general framework for identifying IHL violations. Indeed, the ILC commentary on the Draft Articles repeatedly refers to IHL violations and uses these violations as examples of their implementation. Further, international tribunals have applied a number of the Draft Articles' general principles when determining state responsibility for IHL violations.[720]

With regard to some primary rules, IHL enforces its own accountability systems. In the context of this chapter, there is not notable disagreement between these systems and the Draft Articles. A state's military acts as a state organ and it is in this capacity that militaries engage in armed conflict, as directed by the state.[721] Although in some cases it may be unclear whether a soldier is simply fulfilling their official duties, the in-combat discharge of a weapon is generally attributable to the state. This principle is exemplified[722] by the *lex specialis* of AP I, Article 91:[723] 'a Party to the conflict…shall be responsible for all acts committed by persons forming part of its armed forces',

[719] Rebecca Crootof, 'War Torts: Accountability for Autonomous Weapons' (2016) 164 *University of Pennsylvania Law Review* 1356.
[720] Marco Sassòli, 'State Responsibility for Violations of International Humanitarian Law' (2002) 84 *International Review of the Red Cross* 401, 407.
[721] Their actions are, therefore, within the scope of the Draft Articles: ILC Report 91 [13].
[722] Marco Sassòli, 'State Responsibility for Violations of International Humanitarian Law' (2002) 84 *International Review of the Red Cross* 405.
[723] Marco Sassòli 'State Responsibility for Violations of International Humanitarian Law' (2002) 84 *International Review of the Red Cross* 401, 407.

where '[t]he armed forces of a Party to a conflict consist of all organized armed forces, groups and units which are under a command responsible to that Party for the conduct of its subordinates.'[724] Therefore, should a state's military breach IHL during a conflict, that breach would be easily attributed to the state.[725]

Unclear Attribution: Private Military Contractors

Over the course of the past decade, the use of private military contractors (PMC) has generated a potential responsibility gap. The recent conflicts in Iraq and Afghanistan saw the development of a new trend: military tasks are being increasingly privatised. Formerly a task performed only by soldiers, armed conflict is now partially a PMC task.[726] ACADEMI (previously Blackwater)[727] and similar companies are all symbols of modern, privatised warfare.[728]

With tasks delegated to contracted warriors, Singer refers to this new process as 'military outsourcing and the loss of control.'[729] Within the traditional chain of command, the state maintains disciplinary oversight and command and control over its soldiers. In the case of PMCs, however, hiring states have only contractual relationships with their soldiers.[730] Acts committed by PMCs are attributed to the individuals, rather than to the state. This is true even if the acts include carrying or discharging a weapon.[731] If such acts are performed by PMCs, state responsibility is much lower than it would be for enlisted personnel. This discussion raises three important questions: are PMCs members of the armed forces? PMC employees are neither the

[724] API art 43(1).
[725] Frits Kalshoven, 'State Responsibility for Warlike Acts of the Armed Forces' (1991) 40 *International and Comparative Law Quarterly* 827, also Draft Articles arts 5, 8, 11.
[726] Francesco Francioni, 'Private Military Contractors and International Law: An Introduction' (2008) 19 *European Journal of International Law* 961; Amanda Tarzwell, 'In Search of Accountability: Attributing the Conduct of Private Security Contractors to the United States Under the Doctrine of State Responsibility' (2009) 11 *Oregon Review of International Law* 179; Christopher Lytton, 'Blood for Hire: How the War in Iraq Has Reinvented the World's Second Oldest Profession' (2006) 8 *Oregon Review of International Law* 307.
[727] See <http://academi.com> accessed 15 May 2019; for details on alleged atrocities see: James Glanz & Andrew Lehren, 'Use of Contractors Added to War's Chaos in Iraq' (*The New York Times*, 23 October 2010) <www.nytimes.com/2010/10/24/world/middleeast/24contractors.html?_r=2&hp&> accessed 15 May 2019.
[728] Peter Singer, *Corporate Warriors - The Rise of the Privatized Military Industry* (Cornell University Press, 2003) 157.
[729] Peter Singer, *Corporate Warriors - The Rise of the Privatized Military Industry* (Cornell University Press, 2003) 158.
[730] Francesco Francioni, 'Private Military Contractors and International Law: An Introduction' (2008) 19 *European Journal of International Law* 962.
[731] Carsten Hoppe, 'Passing the Buck: State Responsibility for Private Military Companies' (2008) 19 *European Journal of International Law* 989.

employees of the army nor the employees of the state. Is the PMC contracted to the armed forces or to a State organ? Certainly, the military chain of command exercises management control through the contract. And; who is accountable for any IHL violations, when performed by PMCs? Another possible scenario is when the PMC contracted to a private contractor. In this case, the responsibility of a State is similar to the acts of its nationals or companies incorporated in its territory. Moreover, it is important to establish whether or not a contracting state would be liable for failing to prevent PMC-led violations.

The responsibility for any wrongful acts performed by PMCs should be assigned to whichever organisation holds operational authority.[732] According to Hoppe, hiring states should be given positive obligations and customary international law could allow for PMCs to be assimilated as 'members of the armed forces.'[733] He believes that state responsibility applies to such cases and holds that states should be given a general 'due diligence obligation', forcing them to prevent and suppress IHL and human rights violations.[734] This argument correlates with that presented by Tonkin, stressing the relevance of positive due diligence obligations, should direct attribution fail.[735]

Contracting Phase

In the course of the Contracting Phase, the Hiring State is extremely important as at this point it initiates the action and vets the participants. The Hiring State determines:

- The nature of the activities being outsourced;
- Who will be hired, what licenses they may require, and how they will be screened or vetted;
- Whether the hiring process will be influenced by any historic violations, conduct, or allegation;
- The contract's range (e.g., the confines of its location).

[732] Nigel White & Sorcha Macleod, 'EU Operations and Private Military Contractors: Issues of Corporate and Institutional Responsibility' (2008) 19 *European Journal of International Law* 966.
[733] Carsten Hoppe, 'Passing the Buck: State Responsibility for Private Military Companies' (2008) 19 *European Journal of International Law* 1008.
[734] Carsten Hoppe, 'Passing the Buck: State Responsibility for Private Military Companies' (2008) 19 *European Journal of International Law* 1013.
[735] Hannah Tonkin, *State Control over Private Military and Security Companies in Armed Conflict* (*Cambridge University Press*, 2013) 59.

Many academics and other critics have focused on the fact that individual PMSC operatives are frequently not held criminally accountable for their conduct. However, the allocation of responsibility of providing victims with compensation is just as important in international law and may be a more fruitful field for investigation.

In this section we will examine the relevant sections of international law to assess the ways in which international law deals with, or does not deal with, the broad concept of PMSCs and PMSC personnel being broadly accountable. Following this, a brief outline of recent efforts to support primary analysis will be provided, with the conclusion that the international legal framework as it stands is not effective in providing broad accountability as there is either no legislation or what there is not clear as far as it relates to the legal responsibilities of states or other parties at crucial times.

Recent Developments in the International Legal Framework

The Montreux Document and the U.N. Draft Convention on Private Military and Security Contractors

The Montreux Document, addressing "pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict," comprises two sections.[736] The first section represents a restatement of extant international legal obligations of states interacting with PMSCs and PMSC personnel.

In the first section of the document, considerable clarification is provided regarding a pair of concepts that have remained quite opaque within IHL and IHRL, these being "state responsibility" and "due diligence."

[736] Permanent Representative of Switzerland (Peter Maurer) to the U.N., Letter, October 2, 2008, addressed to the Secretary-General of the Security Council, U.N. Doc. A/63/467-S/2008/636 (October 6, 2008). See Switzerland Federal Ministry of Foreign Affairs, "The Montreux Document on Private Military and Security Companies", available at http://www.eda.admin.ch/eda/en/home/topics/intla/humlaw/pse/psechi.html

The second part of the Document offers "guidance and assistance" to states to assist them to implement their obligations in IHL and IHRL, and also to "[promote] responsible conduct in their relationships with PMSCs operating in areas of armed conflict."[737] The Document, to a greater degree than any extant international law, emphasises the need for domestic/national laws to complement international legal frameworks.

The Montreux document is unique in its approach of taking the state point of view and in introducing the triple-phase construct it highlights the weaknesses in current international law and requirements for domestic laws to fill these. The greatest flaw identified in international law is the fact that it is not able to legislate for the crucial part that the Hiring State plays during the Contracting Phase. The Document does not do much to mitigate this. In Part One, most of the part that addresses the role of the Hiring/Contracting State primarily addresses the In-the-Field and Post-Conduct Phases, targeted at the prevention, suppression, investigation, and prosecution of international humanitarian law/human rights law violations, and remedying "misconduct." [738] There is a single paragraph in the Document that specifically addresses the legal obligations of the Hiring State in the course of the Contracting Phase, stating that a State should not outsource anything subject to international law prohibitions. However, as previously noted, there is very little referring to this problem in IHL, and nothing at all in IHRL.[739]

Contrastingly, the "good practice" in Montreux, which does not represent a legal obligation, encompasses wide-ranging paragraphs related to Determination of Services (i.e., when outsourcing is permissible), Procedure for the Selection and Contracting of PMSCs, Criteria for the Selection of PMSCs, and Terms of Contract with PMSCs. An example of "good practice" would be to have requirements for contracting processes, regulatory frameworks, individual contracts, any incidents that occur, and oversight frameworks to be transparent and public.[740] Two elements emerge from comparing the Document and current law, the first being that international law does not at present impose any legal obligation on states to have specific responsibility during

[737] *Montreux Document*, Part Two.
[738] *Montreux Document*, Part One, secs. 1, 3(c), 4, 6, 8.
[739] *Montreux Document*, Part One, sec. 2.
[740] *Montreux Document*, Part Two, sec. A, II.4

the Contracting Phase, and secondly that domestic legislation may represent the only practical way of imposing such responsibilities.

Montreux does not represent binding law, nor does it detail any novel legal obligation; the UN Draft Convention on Private Military and Security Companies ("Draft Convention") [741] contrastingly, is an attempt to create a completely novel framework in terms of international law specific to PMSCs and their personnel, and will consequently contribute to the soft law in the field. This is attempted through detailing clear state responsibility in extant international law and novel ways of formulating international legal obligations that specifically demand that nations implement legislation regarding a number of elements of PMSC operations. Increasing the coverage of this Draft Convention, it is proposed that the framework should apply at all times rather than, as is the case with Montreux, not just for the duration of an armed conflict, and that it should apply to international organisations.

As previously noted, extant International law is too limited in relation to the Contracting Phase to offer adequate prevention and/or accountability for any violations committed by PMSCs or their personnel. Furthermore, extant International law is frequently unclear or inadequate regarding who is responsible for the regulation of the conduct of PMSCs during the In-the-Field Phase.

Existing international law is especially flawed regarding the Contracting Phase, and the Draft Convention addresses this in several areas. Respecting the question of outsourcing, the Draft Convention offers a broad definition of "inherently state functions", including:

"[D]irect participation in hostilities, waging war and/or combat operations, taking prisoners, law-making, espionage, intelligence, knowledge transfer with military, security and policing application, use of and other activities related to weapons of mass destruction, police powers,

[741] U.N. Human Rights Council, Report of the Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of self-determination, July 2, 2010, U.N. Doc. A/HRC/15/25, Annex ("Draft of a possible Convention on Private Military and Security Companies (PMSCs) for consideration and action by the Human Rights Council").

especially the powers of arrest or detention including the interrogation of detainees and other functions that a State Party considers to be inherently state functions."[742]

Not only does the Draft Convention offer provisions against delegating and/or outsourcing functions that should be undertaken by the state, it further demands that State actors must offer definitions and limitations to the range of activities permitted to PMSCs and to implement legislation, regulations etc for the prohibition of delegating any military/security services to them.[743]

Thus, we can see that the Draft Convention contains measures found nowhere else in international instruments, imposing a definite requirement that national legislation must be implemented that will clarify the phrase "inherently governmental function", and subsequently legislation to prohibit this type of delegation must be introduced. Nevertheless, by offering substantive examples by classifying a number of activities as being inherently state functions, it may be argued that its definitions are too wide ranging as they prohibit outsourcing a substantial collection of activities which includes, for example, intelligence and espionage. It is useful to look at the US, which is noted for providing a substantial proportion of the PMSC industry and also for refusing to support the Draft Convention. The first problem the US has is to accept a definition of "inherently governmental function" that has greater clarity and uniformity than that demanded by domestic legislation passed in 2009. The second problem is that it is well known that the US depends on outsourcing for intelligence and espionage, with up to 30% of US intelligence agency workforces being private contractors.[744] Thus is unsurprising that the US is not keen to support a convention that does not allow intelligence activities to be outsourced. The conflict here represents the real world situation for the US, and the Draft Convention appears to ignore this.

The Draft Convention further covers additional elements of the Contracting Phrase, demanding that PMSC personnel must have training in and be committed to show respect for IHRL and IHL. It is significant that it mandates that Hiring State has responsibility for the implementation of

[742] *Draft Convention*, arts. 2(i), 9.
[743] *Draft Convention*, arts. 4(3), 4(5), 9.
[744] Kristine Huskey and Scott Sullivan, "United States: Law and Policy Governing Private Military Contractors After 9/11," in *Multilevel Regulation of Military and Security Contractors*, ed. Christine Bakker and Mirko Sossai (Oxford, UK: Hart, 2011), 331, 339–41.

legislation and/or regulatory frameworks that guarantee these personnel will be trained in this way.[745] It mandates that state actors must implement additional measures for establishing criteria that will screen PMSC companies and individual personnel, to create licensing frameworks that will be influenced by any reports of human rights abuses, and to create statutory requirements for minimum levels of experience and training for PMSC personnel. [746] These types of obligations and the degree to which they are detailed in the Draft Convention are simply not articulated in existing international law.

The Draft Convention is also unique in that it clearly details and describes the type of substantive international law that would operate in the course of the In-the-Field Phase and also provides clarification for the responsibilities of the state and the state's obligation to exercise due diligence in this phase. An example of this is Article 18 that demands that states should implement legislation or regulations related to the deployment of force and firearms, offering considerable detail as to the times and circumstances in which PMSC personnel may deploy firearms.[747] Regarding state responsibility, it indicates that the States are responsible for all activities related to military/security services of any PMSC that is either operating or is registered within the state's jurisdiction.[748]

An example of this is Article 19, requiring that State actors must ensure that those undertaking "inherently state functions" who commit violations must be punished as criminals under the aegis of national law; any violations of law must be investigated to establish individual criminal responsibility and "no recourse [should be] taken to immunity agreements."[749] With respect to victims of PMSC misconduct, state parties are required to establish legislation or other measures to ensure that ''effective remedies,'' which include restitution, are provided to victims and to ensure that individuals who are found liable, in addition to being subject to ''effective,

[745] *Draft Convention*, arts. 4(2), 15(1)(ii), 14(3), 17(2)–(3), 18(3), 20(1).
[746] *Draft Convention*, arts. 14(3), 16(1)(b).
[747] *Draft Convention*, art. 18.
[748] *Draft Convention*, art. 4(1).

[749] *Draft Convention*, art. 19.

proportionate and dissuasive sanctions,'' also have the obligation to provide restitution or compensation to victims.[750]

The Draft Convention offers considerable detail regarding every element of Contracting phase as it does not only describe what conduct is obligatory and what is prohibited but also offers an explicit requirement for states to implement legislation prohibiting such conduct, additionally demanding specific affirmative action on the part of PMSCs and their personnel. Whilst other human rights instruments have required states to implement domestic legislation to guarantee rights and protections, the Draft Convention offers detail and substance regarding said rights and protections, imposing upon states the burden of introducing domestic legislation that mirrors the Draft Convention's content. This detail may represent both the triumph and the defeat of the legislation.

Including AWS within the ASR Framework

It is important to consider how the responsibility gap might be bridged. To do so, AWS conduct must first be linked to responsible entities. How can elements of the PMC suggestions be applied to AWS?

AWS Conduct and State Responsibility

Should AWS be considered as state organs, as defined by Article 4 ASR, responsibility could be easy to assign. Provided the act in question is performed within an official capacity, state organ responsibility will not be restricted.[751] Unlike humans, AWS would never perform in a private capacity. Despite this, the ASR does not currently classify machines as organs.[752] In turn, AWS are not classified as state organs. Should a machine be classified as an organ, the ASR would become distorted.

[750] *Draft Convention*, arts. 19(4), 20(4); see also art. 23(1).
[751] James Crawford, *The International Law Commission's Articles on State Responsibility - Introduction, Text and Commentaries* (Cambridge University Press, 2002) Art. 4, para 5.
[752] For a definition of state organ: James Crawford, *State Responsibility – The General Part* (Cambridge University Press, 2013) 118; Ronald Arkin, 'The Robot Didn't Do I' (2013) Position Paper for the Workshop on Anticipatory Ethics, Responsibility and Artificial Agents 1.

Nevertheless, AWS misconduct could still be attributable to the state; if an AWS were authorized to perform government-authorised tasks, Article 5 ASR suggests that the state could be responsible for its actions. Offensive attacks are government-authorised acts of violence. However, such attacks, as norms, refer explicitly to a 'person or entity' and are thus intended to specify quasi-state entities.[753] The ASR Commentary further stipulates a 'natural or legal person.'[754] While there has been some debate as to the personhood of robots,[755] there is very limited international support for this notion. Therefore, to apply this definition to AWS would be to stretch the intended application of Article 5.

Article 8 ASR outlines the principle of *de facto* attribution in cases where the act is either state-controlled or state-directed. The wording of this article, however, makes explicit reference to a 'person or group of persons.' It is thus worth considering whether AWS could be considered 'members of the armed forces', as defined by Article 43 of AP I.[756] Regardless, the term 'members of the armed forces' does not apply to machines and, as such, complications persist. This is clear in the reference to 'individuals or persons.'[757] Of particular note, AWS are commanded and operated by human state organs. With this in mind, an attribution link should be established.

State Organ Operators and Responsibility

The actions of military service personnel are considered to be the actions of state organs.[758] Pursuant to Article 4 ASR, the conduct of these individuals is, as such, a state responsibility.[759] Potentially, AWS may disrupt this rule. As yet, it is unclear whether AWS will be commanded or operated by soldiers or military commanders. Therefore, associated conduct could be attributed to

[753] James Crawford, *The International Law Commission's Articles on State Responsibility - Introduction, Text and Commentaries* (Cambridge University Press, 2002) Art. 5, para 1.
[754] James Crawford, *The International Law Commission's Articles on State Responsibility - Introduction, Text and Commentaries* (Cambridge University Press, 2002) Art. 4, para 12.
[755] Andreas Matthisas, *Automata as Holders of Rights. A Proposal for a Change in Legislation* (Logos Verlag, 2010) 37.
[756] In conjunction with Art. 91 AP I it provides a rule of attribution to the state.
[757] Peter Rowe, 'Members of the Armed Forces and Human Rights Law' in Andrew Clapham & Paola Gaeta (eds), *The Oxford Handbook of International Law in Armed Conflict* (Oxford University Press, 2014) 522.
[758] International Court of Justice, '*Case Concerning Armed Activities on the Territory of the Congo (DRC v. Uganda*)', (2005) I.C.J. Reports, 213; see on its customary international law character: International Court of Justice, '*Advisory Opinion - Difference Relating to Immunity from Legal Process of a Special Rapporteur to the Commission of Human Rights*', (1999) I.C.J. Reports, 62.
[759] Ian Brownlie, *Principles of Public International Law* (Oxford University Press, 2018) 450.

either the soldier deploying the AWS, or the commander ordering its deployment. This associated conduct could imply state responsibility.

Preventing Violations as a Due Diligence Obligation

Generally, if unlawful conduct is not directly attributable to a state, the state is not obliged to prevent it.[760] States do, however, have a due diligence obligation to control the use of AWS, and an obligation to avoid wrongful acts. This due diligence demands that states make best efforts to do what is reasonably practicable within their powers, but does not stipulate any specific outcome.[761]

In its *Genocide* case, the International Court of Justice (ICJ) stated that in terms of genocide prevention, states are required to use every reasonably available means, but explained that these attempts do not need to be successful.[762]

Such obligations, according to the ASR Commentary, 'are usually construed as best efforts obligations, requiring states to take all reasonable or necessary measures to prevent a given event from occurring, but without warranting that the event will not occur.'[763] Should a violation occur after a state has failed to take positive prevention measures, this could amount to a wrongful act. Indeed, this failure could amount to state responsibility.[764] Due diligence obligations should be

[760] Jean-Marie Henckaerts & Louise Doswald-Beck, *Customary International Humanitarian Law* (Cambridge University Press, 2005) cit., Rule 149 ('[a] State is responsible for violations of international humanitarian law attributable to it, including: (a) violations committed by its organs, including its armed forces; (b) violations committed by persons or entities it empowered to exercise elements of governmental authority; (c) violations committed by persons or groups acting in fact on its instructions, or under its direction or control; and (d) violations committed by private persons or groups which it acknowledges and adopts as its own conduct').

[761] Pierre Dupuy, 'Reviewing the Difficulties of Codification: on Ago's Classification of Obligations of Means and Obligations of Result in Relation to State Responsibility' (1999) 10 *European Journal of International Law* 371; Riccardo Mazzeschi, 'The Due Diligence Rule and the Nature of the International Responsibility of States' (1992) 35 *German Yearbook of International Law* 47.

[762] International Court of Justice, '*Case Concerning the Application of the Convention of the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) (Merits)*', (2007) I.C.J. Reports, 430; Further see ICJ, '*Case Concerning Armed Activities on the Territory of the Congo (DRC v. Uganda)*', (2005) I.C.J. Reports, 178, applying a standard of vigilance; ICJ, '*Corfu Channel (UK v. Albania)*', (1949) I.C.J. Reports, 22, for a due diligence assessment based on knowledge.

[763] James Crawford, *The International Law Commission's Articles on State Responsibility - Introduction, Text and Commentaries* (Cambridge University Press, 2002) Art. 14, para 14.

[764] Ian Brownlie, *Principles of Public International Law* (Oxford University Press, 2008)150.

considered in terms of a specific, principal obligation.[765] Common Article 1 to the Geneva Conventions (GC) explains that states have an obligation to respect the law of armed conflict (LOAC).[766] Such states are therefore obliged to take careful measures, ensuring that their use of AWS is IHL-compliant. Should a state fail to take such preventative measures, they could be considered responsible for any violations. The *Genocide* case expands upon this, applying a 'psychological element.' It explains that when a 'state is aware, or should normally be aware', it then has an obligation to prevent unlawful conduct.[767] In the case of AWS, the burden of proof is on the state rather than the victims; because of a lack of transparency and for reasons of security, the latter have no access to associated technologies. In such cases, states must take two positive measures to remove their obligations: they must provide a system that is capable of preventing violations and, in a specific case, they must use this system to prevent such violations.

Should a state assist another to perform an internationally wrongful act, they may take on international legal responsibility. Such assistance could, for example, involve the provision of code or hardware. Even if the assisting state does not know that their assistance is unlawful, it must be conscious of the 'factual circumstances' that make them so.[768] For instance, if a state is known to violate IHL through its use of AWS and another state then provides assistance such as associated training, software or hardware, the second state will become internationally responsible for this assistance.

---

[765] Obligations differ for states and circumstances: see Pierre Dupuy, *Due Diligence in the International Law of State Responsibility*, OECD: Legal Aspects of Trans frontier Pollution (OECD, 1977); Riccardo Mazzeschi, 'The Due Diligence Rule and the Nature of the International Responsibility of States' (1992) 35 *German Yearbook of International Law* 30; Jan Hessbruegge, 'The Historical Development of the Doctrines of Attribution and Due Diligence in International Law' (2004) 36 *New York University Journal of International Law and Politics* 265.

[766] Jean-Marie Henckaerts & Louise Doswald-Beck, *Customary International Humanitarian Law - Volume I* (Cambridge University Press, 2009) 509, stating that 'States must exert their influence, to the degree possible, to stop violations of international humanitarian law.'; Birgit Kessler, 'The Duty to Ensure Respect under Common Article 1 of the Geneva Conventions' (2001) *German Yearbook of International Law* 498; for the lack of territorial limitation with regard to Common Art. 1 GC: International Court of Justice, '*Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. USA)*', (1986) I.C.J. Reports, 220, 255; Art. 3 GC IV and Art. 91 AP I reflect as customary law the responsibility of states, see ICJ, '*Case Concerning Armed Activities on the Territory of the Congo (DRC v. Uganda)*', (2005) I.C.J. Reports, 214.

[767] ICJ, '*Case Concerning the Application of the Convention of the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) (Merits)*', (2007) I.C.J. Reports, 431; International Law Commission, Draft Articles on the Prevention of Transboundary Harm from Hazardous Activities with Commentaries (A/56/10, 2001), Art.3, para.18.

[768] Nils Melzer, *Human Rights Implications of the Usage of Drones and Unmanned Robots in Warfare*, European Parliament, Directorate-General for External Policies, 43 (May 2013), *available at* <http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/410220/EXPODROI_ET(2013)410220_EN.pdf.>

It is important, therefore, to consider whether or not AWS autonomy breaches the traditional chain of responsibility. In the case of *Nicaragua v. USA, Nicaragua* argued that the contras were US-funded mercenaries. The ICJ noted that the contras would 'have no real autonomy in relation to [US]' and that, as a result, 'any offences which they have committed would be imputable to [the US].'[769] *Obiter dicta*, these statements could initially suggest that autonomy undermines the traditional responsibility chain. With closer analysis, however, it can be seen that the ICJ does not refer to a weapon's status in terms of the state but, instead, to a group's relationship with the latter. Furthermore, under international law, weapons cannot commit offences. Such violations can only be committed by individuals or states, i.e. humans or human institutions.

In the context of AWS usage, the defence of *force majeure* provides one of the key challenges for state responsibility; Article 23(1) ASR states:

'The wrongfulness of an act of a state not in conformity with an international obligation of that state is precluded if the act is due to force majeure, that is the occurrence of an irresistible force or of an unforeseen event, beyond the control of the state, making it materially impossible in the circumstances to perform the obligation.'

There is an international concern that increasingly autonomous weapon systems will break free of their human control and malfunction. States could thus claim that such events constitute *force majeure* events and avoid any international responsibility for unpredicted IHL violations such as indiscriminate attacks on innocent civilians. Article 32(2)(a) ASR explains, though, that *force majeure* does not apply when 'the situation of force majeure is due, either alone or in combination with other factors, to the conduct of the state invoking it.' The ASR Commentary explains that 'material impossibility cannot be invoked if the impossibility is the result of a breach by that party either of an obligation under the treaty or of any other international obligation owed to any other

[769] *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States)*, ICJ Reports (1986) 14, 64.

party to the treaty.'[770] Therefore, if a state does not take all necessary precautions to ensure that its AWS are IHL compliant (by offering appropriate training for commanders and officers, comprehensively testing systems and ensuring their competent development), it will not be able to claim *force majeure* when an AWS malfunctions or performs in an unforeseen manner. States cannot claim *force majeure* to account for any events that result from their own negligence.[771] Irrespective of the circumstances, the results of human coding and robotic systems do not constitute irresistible forces, nor are their potential malfunctions unimaginable.

Article 23(2)(b) ASR also explains that a state cannot claim *force majeure* if it 'has assumed the risk of that situation occurring.' Crawford further explains this notion, stating that '[i]f a state accepts responsibility for a particular risk, it renounces its right to rely on *force majeure* to evade that responsibility. It may do so expressly, by agreement, or by clear implication.'[772] Should a state accept the risk of operating an AWS that is known to be defective or ineffective, that state is then responsible for any of its unexpected operations; in such cases, the AWS' use is said to have a level of predictable unpredictability.[773] As such, any state that operates these technologies on the battlefield and seeks to benefit from their operation will also accept any associated risks. A particularly complex question is that of AWS hacking and whether states can claim *force majeure* from any subsequent violations. Hacking is, however, a common countermeasure and, arguably, this is a risk that all states accept when using the cyber domain for warfare. As such, states retain their responsibility for AWS actions, even in very extreme circumstances.

The Removal of Human Judgement

According to Beard, 'the elusive search for individual culpability for the actions of [AWS] foreshadows fundamental problems in assigning responsibility to [S]tates for the actions of these

[770] Articles on the Responsibility of States for Intentionally Wrongful Acts, in Report of the International Law Commission to the General Assembly on Its Fifty-Third Session, 56 U.N. GAOR Supp. No. 10, at 1, 43, U.N. Doc. A/56/10 (2001) art. 23, § 9.
[771] James Crawford, *State Responsibility: The General Part* (Cambridge University Press, 2014) 298.
[772] James Crawford, *State Responsibility: The General Part* (Cambridge University Press, 2014) 301.
[773] Robin Geiss, *Autonomous Weapons Systems: Risk Management and State Responsibility*, Presentation, Informal Meeting of Experts on Lethal Autonomous Weapons Systems of the Convention on Certain Conventional Weapons (CCW) (April 2016) *available at* <http://www.unog.ch/80256EDD006B8954/(httpAssets)/00C95F16D6FC38E4C1257F9D0039B84D/$file/Geiss-CCW-Website.pdf.>

machines.'[774] He considers that both individual and state responsibility for attacks are based on human judgement:

'Legal and political accountability flows from the judgments of commanders [in meeting the requirements of IHL]. Not only is it necessary that a human make this judgment, but increasingly (under the applicable policies of [S]tates), a human at the highest levels of authority must make this judgment…'[775]

From this perspective, should an AWS be so autonomous that no state organ applies human judgement to its control, the legal obligation for human judgement, as stipulated by the law of state responsibility, is unfulfilled.

Beard's argument, however, is founded on a flawed idea that state responsibility relies on a human directly controlling an attack, as seen in the use of manual weapons. As noted by Schmitt, '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 [AWS].'[776] Weapon systems developers, attack planners and others military personnel all contribute to the use of AWS in military attacks. Their involvement provides a link to the state, determining state responsibility for AWS-inflicted harm. Further, references to human judgement incorrectly suggest a requisite mental element within state responsibility; as the ILC explains in its Commentary to Draft Article 2, '[i]n the absence of any specific requirement of a mental element in terms of the primary obligation, it is only the act of a state that matters, independently of any intention.'[777] No such mental element is stipulated by any of the obligations borne by military personnel when planning or executing attacks or discharging a weapon. It can therefore be concluded that states are responsible for any AWS-performed action, regardless of the level of associated human judgement. In this regard, the international law of state responsibility imputes strict liability.

---

[774] Jack Beard, 'Autonomous Weapons and Human Responsibilities' (2014) 45 *Georgetown Journal of International Law* 617.
[775] Jack Beard, 'Autonomous Weapons and Human Responsibilities' (2014) 45 *Georgetown Journal of International Law* 675.
[776] Michael Schmitt, 'Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics' (2013) *Harvard National Security Journal* Features 33.
[777] Report of the International Law Commission, UN GAOR, 56th sess, Supp No 10, UN Doc A/56/10 (2001) ('ILC Report') 73 [10].

This thesis disagrees with Beard on a number of counts. Beard appears dependent on the notion that advanced AWS represent something other than a simple weapon system. This is shown in his suggestion that AWS may make decisions about legal adherence. Further, he appears to ignore the role of human commanders, their decision to deploy AWS within specific circumstances, and the legal burden associated with this human decision.

Classifying AWS as State Agents

While the notion of a state agent is case specific, there are some explicit rules and clear interpretations. ASR outlines the most apparent issues regarding the definition of a state agent.[778] The primary rules stipulate that if an individual and state organ is legally empowered to exercise governmental authority and performs its tasks on behalf of a state,[779] any resulting actions will be considered state acts.[780] In fact, it is sufficient for an individual or group to be acting under the direct control, or upon the instructions, of a state.[781] In such circumstances, states are responsible for resulting acts even if the state organ 'exceeds its authority or contravenes instructions.'[782] Further, ASR includes a provision for scenarios in which acts are conducted without official authorities:

'The conduct of a person or group of persons shall be considered an act of a state under international law if the person or group of persons is in fact exercising elements of the governmental authority in the absence or default of the official authorities and in circumstances such as to call for the exercise of those elements of authority.'[783]

In terms of AWS, the AWS is not the State agent but the person who decides to use an AWS is a State agent. The most significant issue is that humans always create the attribution conditions. As such, attribution does not result from the system itself but, instead, from its human operator.

[778] Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries: 2001, (hereinafter ASR) (ILC Yearbook 2001, vol. II[2]).
[779] Art 4(1-2), ASR.
[780] Art. 5, ASR.
[781] Art. 8, ASR.
[782] Art 7, ASR.
[783] Art. 9, ASR.

Further, the articles explain that a state can accept an act as its own responsibility, even if the act would not otherwise be attributable to the state.[784] Circumstances such as these provide some of the clearest attribution examples. In conclusion, the actions of regular citizens are not normally attributable to a state.

Attribution will change if state organs are detached to another state and placed at its disposal. In specific, limited cases such as this, the state organ's actions then become attributable to the new state.[785] Finally, the articles also regulate attribution during revolutions or similar movements.[786] Such scenarios would also imply an associated change in the attribution of AWS operators.

The principal rules of attribution are, therefore, simple. The issue itself forms the primary focus of the secondary norms of state responsibility doctrine. Attribution is necessary for international wrongful acts[787] and if an act is performed by a state organ or individual with official duties, such attribution will occur.[788] It is important to note that a state acts can also concern omissions.[789] In the realm of AWS, omissions could be as likely as positive actions. As such, even in cases where the rule of attribution is evident, state acts and actors are always defined independently.[790] It seems that in the context of AWS, analysis is even more relevant; machines do not constitute state agents and, as such, do not perform *de jure* acts of state. Appropriate explanations can be seen in similarly technological areas of law, such as international cyber law.[791] Within the field of cyber warfare, NATO's international law specialists have applied the rule of attribution.[792] According to the resulting *Tallinn Manual*, the simple fact that an act is performed by means of a (cyber) system

[784] Art. 11, ASR.
[785] Art. 6 and Commentaries (1-9), ASR.
[786] Art. 10, ASR.
[787] Art. 2., ASR.
[788] Art. 4., ASR.
[789] Art 2, ASR.
[790] Claim of the Salvador Commercial Company (El Triunfo Company), Volume XV RIAA (1902) 468-479 at 476-477; *D. Earnshaw and Others (Great Britain) v. United States* (Zafiro case) Volume VI, RIAA (1925) 160-165 at 163-165.
[791] See more e.g. Ian Lloyd, *Information Technology Law* (Oxford University Press, 2011).
[792] International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, in Michael Schmitt General (eds), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press: Cambridge, 2013) Rule 6, at 29-34.

does not automatically prove attribution.[793] Similar principles have already been applied in policy guidance for AWS.[794] Certainly, there must be an individual of group of individuals who represent state responsibility and such technologies only identify these individuals. In some real-life situations, establishing attribution will be more difficult than others; this will depend on the AWS in question.

Consequently, and in accordance with ASR, AWS do not constitute state agents.[795] When using AWS, the state agent will be whoever acts in the capacity of a state, as outlined above. As machines cannot legally represent a state in the way that a human can, the status of the AWS operator will determine whether or not state responsibility doctrine is applicable. What is apparent, is that the level of autonomy held by an AWS will strongly influence the identification of this individual. In every context, the role of the state agent will change.

At the third level, *human off the loop,* the AWS has no direct connection with its associated state agents. This stretches and complicates the nexus. There are three key aspects of these scenarios that should be considered: the human who activates the system; the AWS' command structure; and the manufacturer and owner of the AWS, when employed as a state actor. The closest link with a *human off the loop* AWS is its human activator. There is a strong argument to suggest that the activator, as the last human who has contact with the AWS, would meet the criteria provided by Article 4, 5 or 8 ASR, according to the specific situation. If it were accepted that only the sender or activator would constitute a state agent, responsible for the AWS, then AWS acts would be considered acts of the relevant state.[796] This approach will be henceforth referred to as the last human theory.

It is also important to consider the other aspects. The command structure of a *human off the loop* AWS must be examined separately. Clearly, structural analysis is relevant to state agent analysis.

[793] International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, in Michael Schmitt General (eds), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Rule 7-8, at 34-35.
[794] Artur Kuptel, and Andy Williams, Policy Guidance: Autonomy in Defence Systems (29 October 2014). Available at SSRN: <https://ssrn.com/abstract=2524515> accessed 27 February 2020, 16.
[795] Artur Kuptel, and Andy Williams, Policy Guidance: Autonomy in Defence Systems (29 October 2014). Available at SSRN: <https://ssrn.com/abstract=2524515> accessed 27 February 2020, 18.
[796] Arts. 1-4, ASR.

In accordance with ASR, state organ conduct is that which 'exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the state.'[797] As such, it is clear that acts within a command chain are official state acts. In situations where the command structure is attached to a different state than the last human, the allocation of attribution is complicated. There is no one-size-fits-all solution. ASR does, however, provide a small number of possibilities. One such possibility is that of joint responsibility.[798] In these circumstances, both states would be considered to own the act in question and, as such, be accountable for the internationally wrongful act. In other cases, operators could be fully adopted into the command structure of the new state.[799] In this scenario, the operator would be seen as a state actor for the new state, and their actions would not constitute any act by the original state. In such situations, the new state would be automatically responsible for any internationally wrongful acts committed by the operator. It is thus arguable that command structure holds more weight than the last human theory. This rule does not apply in cases of *ultra vires* acts, committed by a human actor.

Ownership of an AWS is closely related to the operator and the command structure. An AWS owner will most likely be at least complicit in its actions, including any internationally wrongful acts. In these circumstances, owners could be considered accountable, either because they are the operator or for reasons pertaining to the AWS' command structure. This would be true unless they had handed the system over to a new owner or its control had been taken away. In the first instance, AWS owners would become either a former owner or a machine lender. ASR makes no specific provision for sales in terms of the secondary norms of state responsibility. Likewise, if an AWS is lent to another party, it constitutes nothing more than an item of technology, regulated by the lease agreement. Such agreements would not affect the overarching rule of attribution and the new operator would be limited by its own specific obligations. Sales are regulated by primary norms. When these rules are followed, however, state responsibility doctrine does not apply to a machine's seller or lender. AWS theft could pose significant issues for the owner. However, if a state had taken appropriate measures to protect its machines from theft, it would not then be accountable for any subsequent actions taken by the stealing agent. Conversely, negligence could see state

[797] Art. 4, ASR.
[798] Art. 47, ASR.
[799] Art. 6, ASR.

responsibility rise to that of an internationally wrongful act. These remain system-specific primary norm obligations and do not apply to every AWS. Accordingly, the AWS owner role adds nothing new to the secondary norm element of state responsibility. However, if the commercial agreements made between states are breached, this could lead to an internationally wrongful act. Typically, though, the transfer of goods and services will have *lex specialis* doctrines to cover the matter.

In summary, there is a clear link between the existence of a state agent and state attribution. This nexus serves as a firm foundation for state responsibility doctrine. Should wrongful acts be committed by state organs, these acts will then be attributable to the state.

Can a Stricter Liability Regime Overcome Potential Accountability Gaps?

The problem can be illustrated by considering the following case: A military leader puts a rigorously tested and fully authorised autonomous weapons system into the field. This system operates autonomously in a multifaceted and rapidly changing frontline environment, and it unpredictably acts in violation of the laws of armed conflict such as targeting civilians based on wrong algorithms. There is no evidence to suggest that the military leader acted with intent or negligence. Furthermore, as intent and negligence represent human mental states, by their nature, they are not manifest in a robot. In addition, in light of the intricacy of these systems, it could be challenging to ascertain exactly what went wrong. Accordingly, if the principal question relies on an element of fault, it could be difficult to ascertain or substantiate that the responsibility lies with the state.

To deal with this particular challenge, there is a requirement to develop a rule for autonomous weapons systems that does not rely on proof of fault (strict liability), or to reverse the burden of proof (presumed liability). However, it is important to note that the feasibility of implementing a liability regime of this nature within the sphere of the laws of armed conflict are remote. Strict liability (which is also referred to as absolute liability or operator's liability) entails removing the question of fault (negligence, recklessness, intent) from the deliberation. Responsibility is routinely generated at the point at which the risks that are intrinsic in unpredictable robotic behaviours come into fruition. Within the confines of such a stringent liability regime, it is immaterial what the operator, programmer, military commander, or state that commissioned the

robot anticipated it would do, all that is of relevance is what the AWS actually did. The extent to which the actions can be traced back to a failure of the sensors, an interference from an external party that had not previously been anticipated, variations in the operating conditions, a coding bug, or software issues, is immaterial.

Strict liability regimes are not unusual when addressing dangerous activity and highly complex procedures that could entail that it is fundamentally challenging to pinpoint and substantiate where the errors lie.[800] From a domestic perspective, product liability systems frequently rely on strict liability. From an international perspective, with the exception of *the ILC Draft Principles on the Allocation of Loss in the Case of Transboundary Harm Arising out of Hazardous Activities*,[801] the *Outer Space Treaty 1967* and *the Space Liability Convention 1972*—evident interpretation challenges put aside—are ideal examples. Article VII of *the Outer Space Treaty* states, '[e]ach State Party to the Treaty that launches [...] an object into outer space [...] is internationally liable for damage to another State Party to the Treaty [...].' [802] The concepts that informed the implementation of this liability system are, in multiple regards, comparable to the areas of relevance when considering AWS. *The Outer Space Treaty* was drafted and implemented during the 1960s, a period during which there was a lack of understanding of space-based technologies and they were viewed with a jaundice eye due to their inherent complexity. In the contemporary era, we find ourselves viewing AWS in much the same light. Expectedly, strict liability systems are in the process of being debated on a domestic level that specifically address the civil applications of autonomous technologies.

As well as overcoming the very particular responsibility issues associated with high-risk, volatile and multifaceted mechanisms, the implementation of a strict international liability system would engender convincing enticements to deploy AWS with caution, to perform in-depth reviews of

[800] *Trail Smelter Arbitration (United States v. Canada)* Arbitral Tribunal, 3 U.N. Rep. International Arbitration Awards 1905 (1941).
[801] According to Principle 4 ('Prompt and adequate compensation') of the ILC Draft Principles on the Allocation of Loss in the Case of Transboundary Harm Arising out of Hazardous Activities: 'Each State should take all necessary measures to ensure that prompt and adequate compensation is available for victims of transboundary damage caused by hazardous activities located within its territory or otherwise under its jurisdiction or control. These measures should include the imposition of liability on the operator or, where appropriate, other person or entity. Such liability should not require proof of fault.'
[802] (Article II 1972 Liability Convention).

systems, implement actions to reduce risk, code AWS conservatively, and put in place stringent product liability regimes on a domestic level.

There is a need for further consideration of the ways in which a liability regime of this nature could be implemented in the setting of an armed conflict in the context of technologies that are, by their very nature, intended to legally cause damage. The accountability rules outlined in *the Outer Space Treaty* and *Space Liability Convention*, which assert that a state is wholly liable for the Earth-based damage that can be traced back to its space objects, are clearly not directly applicable to AWS. As such, AWS need a more intricate liability system that is directly applicable to the unpredictable and specific nature of an armed conflict. On balance, within armed conflict situations, certain damage can be expected; for example, the obliteration of a military target, and such destruction is undoubtedly admissible during armed conflict. Furthermore, it does not induce state responsibility. Furthermore, the unpredictability and risks that are inherent within AWS could be of a more significant issue in some cases (for example, when utilised in a municipal area) than they are in others (for example, when they are deployed in a military training zone or in space). As such, a tiered liability system could be relevant through which stringent or apparent liability is enforced in some cases with regard to certain, fundamental rules, but not in all cases and not to support affecting damage on a general level, or in the context of the full gamut of rules that govern the laws of armed conflict. Aa graduated liability scheme of this nature would amalgamate strict liability with alternative aspects of liability and, as such, could have the ability to respond to the unique nature of the risks and ambiguities that are intrinsic in AWS.[803]

Accountability in Domestic Courts

In order for a state to be held accountable for international law violations made by its AWS, it must have a legal entity, such as a court, which it can answer to. Further, the individual victims or victim state must actively challenge the offending state's behaviour. This section will examine

[803] Nehal Bhuta & Stavros Pantazopoulos, 'Autonomy and Uncertainty: Increasingly Autonomous Weapons Systems and the International Legal Regulation of Risk in Nehal Bhuta, Susanne Beck, Robin Geiβ, Hin Liu, & Claus Kreβ (eds), *Autonomous Weapons Systems: Law, Ethics, Policy* (Cambridge University Press, 2016) 290; Robin Geiss, and Henning Lahmann, 'Autonomous Weapons Systems: A Paradigm Shift for the Law of Armed Conflict' in Jens David Ohlin (eds), *Research Handbook on Remote Warfare* (Edward Elgar, 2016) 391.

whether domestic courts might offer an effective forum for victim-instigated legal cases caused by AWS use.

Although victim states will typically have more resources with which they can file against offending states, individual victims may, theoretically, be able to take them to domestic court. This option is, however, far from practical. The victims of such crimes are typically impoverished and some geographical distance away.[804] Using this type of accountability, victims would be burdened with filing action against offending state governments and would be required to do so with almost no resources. With opponents of this nature, individual victims would be unlikely to take on such a burden, especially after having already suffered the impact of the initial crime. This is, of course, assuming that the victims even know that they have such rights. In some cases, however, it is possible that victims might have the resources to challenge offending states, especially if they have NGO support and the offending state is subject to strict liability for AWS violations. This subsection will consider the legal viability of an individual using the domestic courts to file against a state.

For a victim to bring suit, they must first gain access to a court. There would be two possible options. Firstly, they might decide to address the matter in a foreign court, assuming that the corresponding domestic law would consider such cases. Very few states provide civil remedies for extraterritorial torts.[805] As such, should an US-owned AWS harm a victim in Pakistan, for example, and in doing so violate international law, that victim would be challenged to find a foreign court which would entertain the case. To circumvent this issue, many states allow victims to attach their civil claims to ongoing criminal prosecutions for overseas crimes.[806] However, this method would not allow victims to hold the state to account. For instance, victims cannot bring civil proceedings against State A in the court of State B on account of sovereign immunity.

[804] *Al-Skeini and others v. United Kingdom* App. No. 55721/07, 7 July 2011: *Al-Jedda v. United Kingdom* App. No. 27021/08, 7 July 2011. Human Rights Watch, Losing Humanity: The Case Against Killer Robots 3 (2012), available at <http://www.hrw.org/sites/default/files/reports/arms111 2ForUpload_0_0.pdf> accessed 27 February 2020, 44.
[805] Beth Stephens, 'Translating Filartiga: A Comparative and International Law Analysis of Domestic Remedies for International Human Rights Violations' (2002) 27 *Yale Journal of International Law* 4.
[806] Beth Stephens, 'Translating Filartiga: A Comparative and International Law Analysis of Domestic Remedies for International Human Rights Violations' (2002) 27 *Yale Journal of International Law* 17, 18.

Essentially, foreign courts are unlikely to provide a suitable forum in which victims can hold offending states to account for their actions.

The second option would be for victims to file against the offending state in their own domestic courts. In order to do so, domestic law would need to provide a suitable cause of action, such as a tort.[807] While in many states an international crime does not, by default, trigger a domestic cause of action,[808] the harm that is likely to result from AWS violations (property damage, bodily injury, and death) is likely to be covered by tort law. Therefore, it will often be the case that victims have a cause of action to support their case.[809]

Nevertheless, sovereign immunity will present an even greater obstacle for any individual victim who chooses to pursue this route. The doctrine of sovereign immunity generally shields states from any liability in foreign courts. However, this obstacle could potentially be overcome. Although sovereign immunity was once absolute,[810] it now has a wide range of associated exceptions;[811] most significantly, there is a territorial tort exception. This exception allows legal professionals within a state to sue foreign governments for torts that occur with the former's territory.[812] This mechanism has become increasingly popular in recent years[813] and may enable actions for AWS violations, with many such international crimes also constituting domestic torts.

[807] Bahareh Mostajelean, 'Foreign Alternatives to the Alien Tort Claims Act: The Success or Is It Failure? of Bringing Civil Suits Against Multinational Corporations That Commit Human Rights Violations' (2008) 40 *The George Washington International Law Review* 497.
[808] Beth Stephens, 'Translating Filartiga: A Comparative and International Law Analysis of Domestic Remedies for International Human Rights Violations' (2002) *Yale Journal of International Law* 31.
[809] See *Xuncax v. Gramajo*, 886 F. Supp. 162, 183 (D. Mass. 1995).
[810] Adam Belsky, Mark Merva & Naomi Roht-Arriaza, 'Implied Waiver Under the ESIA: A Proposed Exception to Immunity for Violations of Peremptory Norms of International Law' (1989) 77 *California Law Review* 377, 379.
[811] MPA Kindall, 'Immunity of States for Non-commercial Torts: A Comparative Anaysis of the International Law Commission's Draft' (1987) 75 *California Law Review* 1849.
[812] This exception allows actions against states that relate to 'death or injury to [a] person, or damage to or loss of tangible property, caused by an act or omission which is alleged to be attributable to the State, if the act occurred in whole or in part in the territory of that other State and if the author of the act or omission was present in that territory at the time of the act or omission.' U.N. Convention on Jurisdictional Immunities of States and Their Property, art. 12, G.A. Res. 59/38, (Dec. 2, 2004).
[813] For example, State Immunity Act, c. 33, § 6 (1978) (U.K.); State Immunity Act, R.S.C., c. S-18 (1985) (Can.); State Immunity Act of 1985, c. 313, § 7 (1985) (Sing.); Foreign Sovereign Immunity Act of 1981, art. 6 (1981) (S. Aft.). Moreover, twenty-eight states have ratified the U.N. Convention on Immunities, which also includes the exception.

What is unclear, however, is whether this exception would always prevent sovereign immunity for AWS violations committed within the victim state territory. Historically, its use has been limited to private or managerial state activities (*acta jure gestionis*), and such activities tend to be commercial.[814] Conversely, it has not been applied to sovereign acts (*acta jure imperil*) which, as typically public acts, include military activity.[815] For instance, in Singapore and the U.K., the territorial tort exception clearly exempts any foreign military acts.[816] Similarly, some national courts have declared immunity for military and public actions, irrespective of any exception that may already have existed.[817] Moreover, through ratification of the European Convention on State Immunity or the U.N. Convention on Immunities, several states have plainly stated that the territorial tort exception is not applicable to their military actions.[818]

On account of the factors listed above, the ICJ concluded in *Jurisdictional Immunities of the State* that states may still assert sovereign immunity in foreign courts for public acts, including military action during an armed conflict. The conclusion affirms that this is true even in cases where the territorial tort exception might, otherwise, be applicable.[819] In contrast, it explains that customary international law demands that 'a state be accorded immunity in proceedings for torts allegedly committed on the territory of another state by its armed forces and other organs of state in the course of conducting an armed conflict.'[820] Further, it clarifies that sovereign immunity remains extant even in cases whereby a state's actions have violated international law. This position rejects

[814] *Jurisdictional Immunities of the State (Germany v. Italy: Greece Intervening), Judgment*, T 64 (Feb. 3, 2012), available at http://www.icj-cij.org/docket/files/ 143/16883.pdf.
[815] Sevrine Knuchel, 'State Immunit and the Promise of Jus Cogens' (2011) 9 *Northwestern University Journal of International Human Rights* 154.
[816] State Immunity Act, c. 33, 5 6 (1978) (U.K.); State Immunity Act of 1985, c. 313, 5 7 (1985) (Sing.).
[817] *Jurisdictional Immunities of the State (Germany v. Italy: Greece Intervening), Judgment*, 72-75 (Feb. 3, 2012), available at http://www.icj-cij.org/docket/files/ 143/16883.pdf (describing decisions of courts in Egypt, Belgium, the Netherlands, Italy, the U.K., Ireland, France, Slovenia, Poland, Brazil, and Germany).
[818] *Jurisdictional Immunities of the State (Germany v. Italy: Greece Intervening), Judgment*, 72-75 (Feb. 3, 2012), available at http://www.icj-cij.org/docket/files/ 143/16883.pdf (noting that Belgium, Ireland, Slovenia, Greece, Poland, Norway, and Sweden have declared the territorial tort exception inapplicable to the acts of foreign states' armed forces).
[819] *Jurisdictional Immunities of the State (Germany v. Italy: Greece Intervening), Judgment*, 78 (Feb. 3, 2012), available at http://www.icj-cij.org/docket/files/ 143/16883.pdf.
[820] *Jurisdictional Immunities of the State (Germany v. Italy: Greece Intervening), Judgment*, 78 (Feb. 3, 2012), available at http://www.icj-cij.org/docket/files/ 143/16883.pdf.

the claim that a state will surrender its immunity if ever it is 'accused of serious violations of international human rights law or the international law of armed conflict.'[821]

The ICJ ruling indicates that international law would bar citizens from suing foreign states for public actions during armed conflict, even if their domestic laws might permit them to do so. Most likely, this will prevent individuals using their domestic courts to hold offending states to account for AWS crimes committed during a conflict. Of relevance, though, the ICJ clearly limited its decision to crimes committed 'in the course of conducting an armed conflict.'[822] Therefore, it is arguable that for any military action conducted outside of an armed conflict, states would not have immunity. Therefore, domestic courts might still serve to adjudicate AWS crimes, provided they occur outside of this context.

The context of an AWS' use will thus determine whether or not the victim's domestic courts can viably rule on liability. AWS will, no doubt, be employed during armed conflicts and, as such, states will likely be immune for any resulting crimes. Conversely, should a state employ an AWS beyond the scope of an armed conflict, victims would likely be able to sue the offending state, aided by the territorial tort exception. Should AWS be used in the same manner as drones, striking terrorists found beyond the geographical parameters of a conflict, immunity will depend on whether the court in question deems counterterrorism operations to be within the scope of that conflict. The utility of domestic courts for private actions will thus be determined by the context in which the offending AWS was used.

Under international law, it may therefore be possible for individual victims to hold offending states to account in their own domestic courts. For instance, *Al-Skeini and others v. United Kingdom* and *Al-Jedda v. United Kingdom* cases that have been brought in England arising out of the behaviour of the armed forces during armed conflict and outside national territory. It should be noted that they were only possible due to the Human Rights Act.[823] This opportunity, however, is unlikely to

[821] *Jurisdictional Immunities of the State (Germany v. Italy: Greece Intervening), Judgment*, 91 (Feb. 3, 2012), available at http://www.icj-cij.org/docket/files/ 143/16883.pdf.
[822] *Jurisdictional Immunities of the State (Germany v. Italy: Greece Intervening), Judgment*, 65 (Feb. 3, 2012), available at http://www.icj-cij.org/docket/files/ 143/16883.pdf.
[823] *Al-Skeini and others v. United Kingdom* App. No. 55721/07, 7 July 2011: *Al-Jedda v. United Kingdom* App. No. 27021/08, 7 July 2011.

render domestic courts a suitable or practicable forum for establishing state liability. They are of course limited forums and, as such, actions will not be possible if crimes are committed within the scope of an armed conflict. Given that AWS usage will most commonly occur during periods of armed conflict, states will, in most cases, hold sovereign immunity.

Moreover, even without this limitation, there are a number of practical challenges that could prevent such cases coming to court. In most cases, individual victims will not have the resolve, sophistication or resources to bring a foreign state to trial.[824] For cases that do arise, victims may struggle to encourage the offending state to appear in the victim's own domestic court. Further, any resulting judgement may be even harder to enforce.[825] Therefore, the use of domestic courts would, in most cases, be ineffective. Together with the limitations of sovereign immunity, these challenges mean that domestic courts are largely unable to rule on state liability for AWS crimes.

Conclusion

A review of the existing literature on AWS indicates that the concept of State responsibility has yet to attract significant attention. This can potentially be attributed to the fact that it would be less problematic than the idea of individual criminal responsibility.[826] As such, once it has been established that a State actor has deployed an AWS, the State would be held accountable if the infliction of the harm violated relevant international law and that generally requires some form of fault. Furthermore, any unanticipated malfunction could be entreated as a *force majeure* impeding wrongfulness: According to the law of State responsibility, *force majeure* is not sufficient to excuse any violation of a definite standard of international law, a category that undoubtedly incorporates central norms of international humanitarian law; for example, the principles of proportionality and distinction.[827]

[824] Human Rights Watch, Losing Humanity: The Case Against Killer Robots (2012), available at <http://www.hrw.org/sites/default/files/reports/arms111 2ForUpload_0_0.pdf> 44.
[825] MPA Kindall, 'Immunity of States for Non-commercial Torts: A Comparative Analysis of the International Law Commission's Draft' (1987) 75 *California Law Review* 1862, 1872.
[826] Human Rights Watch (HRW) and Harvard's International Human Rights Clinic (IHRC) (2015) *Mind the Gap. The Lack of Accountability for Killer Robots* 13.
[827] Nils Melzer, *Human Rights Implications of the Usage of Drones and Unmanned Robots in Warfare* (2013) Bruxelles: EU Directorate-General for External Policies 40.

A categorical positivity of this nature is completely uncorroborated. That is, any assumption that State accountability for any IHL violations would not incorporate the establishment of some form of mental element is erroneous. While fault is not considered to represent a constitutive aspect of State responsibility according to general international law, it is also rather uncontentious that the significance of a blameworthy mental aspect may be envisioned by the primary norm whose purported violation is at stake. This is specifically the case of IHL policies. The rule that inhibits forces launching a direct attack on a civilian population, for example, debatably assumes that there is an aspect of intentionality. If an attack that is launched as a result of a malfunction causes civilian harm, such an attack does not represent a breach of the standard of distinction because the State did not directly take action that targeted civilians.

As such, the unpredictable nature of AWS encumbers the establishment of individual criminal responsibility, State responsibility will be equally problematic. In this regard, State responsibility does not represent a legal cure-all that can adequately address the responsibility issues associated with AWS. It is worth noting that the scholars who have taken a more optimistic stance in this regard appear to comprehend the law of State responsibility in the context of internationally unlawful acts as a no-fault accountability system.[828] This is erroneous *de lege lata*, as States can potentially avoid taking accountability if they effectively call on *force majeure* to excuse themselves from culpability. However, the introduction of a strict liability rule pertaining to civilian harm—for example, the 1972 Convention on the International Liability for Damage Caused by Space Objects—unquestionably represents a promising possibility from the *de lege ferenda* viewpoint.

But what are the implications in terms of the current standing of the law of State responsibility? It would be an oversight to suppose that it is not of relevance in the pursuit of a solution to eradicate the AWS-related responsibility gap. Indeed, although fault represents a fundamental aspect of IHL violations, there is an IHL standard that sets the bar for the mental aspect at an acutely low level; that is, the norm of precaution during attacks, which asserts that

[828] Robin Geiss, and Henning Lahmann, 'Autonomous Weapons Systems: A Paradigm Shift for the Law of Armed Conflict' in Jens David Ohlin (eds), *Research Handbook on Remote Warfare* (Edward Elgar, 2016) 386.

'[e]ach party to the conflict must take all feasible precautions in the choice of means and methods of warfare with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects.'[829]

The concept of 'all feasible precautions' debatably involves some form of due diligence, which could be infringed by a negligent (or at least irresponsible) behaviour.[830] Unlike the principle of command responsibility, the principle of precaution does not assume that human subordinates have commissioned war crimes. Rather, it exclusively refers to 'the choice of means and methods of warfare.' This necessitates that, according to the principle of precaution, the negligent utilisation of an AWS that leads to civilian losses could fall under the domain of State responsibility, even if it is not possible to establish direct criminal responsibility.

[829] Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law* (Cambridge University Press, 2005) 56.
[830] Yael Ronen, 'Avoid or Compensate? Liability for Incidental Injury to Civilians Inflicted During Armed Conflict' (2009) 42 *Vanderbilt Journal of Transnational Law* 185.

Chapter 7 - Individual Responsibility and Autonomous Weapon Systems

Introduction

Modern war technologies include a growing range of Autonomous Weapons Systems (AWS). These systems are programmed for target selection and engagement without human authorisation or intervention. They pose a significant challenge for the principles of International Humanitarian Law (IHL) and could spark an increase in international conflict and accountability problem during conflict. Opponents of such AWS hold that any weapon system that acts independently will effectively break away from its chain of command.[831] The important question, therefore, is who is ultimately responsible for the actions of the system when things go wrong and a war crime is committed. Those who are potentially liable for the actions of such systems, including programmers, the State, military commanders, manufacturers or, indeed, the system itself.

This chapter consists of three sections. Section one considers how can we attribute responsibility to a large group of programmers being involved in the development stage of AWS algorithms? Section two examines whether commanders have effective command and control over AWS in the battlefield and can AWS be part of a hierarchical system and disciplined by their commanders?

[831] Daniele Amoroso and Benedetta Giordano, 'Who Is to Blame for Autonomous Weapons Systems' Misdoings?' in Elena Carpanelli and Nicole Lazzerini (eds), *Use and Misuse of New Technologies* (Springer, 2019) 225.

Finally, section three evaluates whether the corporation will be responsible for the acts of its human agents?

AWS Programmer Liability

To a significant extent, the behaviour of an AWS is influenced by development work conducted prior to its deployment. As with any other modern weapon system, the development of an AWS is highly complicated. It sees continual input from sizeable teams of individuals and organisations. The specification stage will be driven by military decision makers, liaising extensively with system producers who then respond to the given specifications. Further, there will be significant interaction between these parties and those who are charged with the system's testing, approval, production and delivery. In the context of this section, programmers are the individuals who influence the behaviour of the AWS. Operators, conversely, are those responsible for its use in armed conflict.

Unlike other weapon programmers, the role of an AWS programmer is not necessarily consistent with existing legal frameworks. Not only will such programmers influence the capabilities of the system, but they could also control the specific actions it performs when deployed. The extension of this influence stems from the way in which the AWS control system 'steps into the shoes' of a human operator, minimising their influence and requirement. On account of this, an AWS programmer's influence is placed somewhere between the soldier and AWS activation. Broadly, systems with greater autonomy will reduce the control ability of their in-field operators and, in turn, increase the control ability of their programmers.[832]

If AWS autonomy ranges from complete human control, though levels of shared control, to complete autonomy, it is important to consider any circumstances in which a system's integral autonomy and associated programmer activity might influence attribution for serious IHL violations.[833] Of course, a key requirement would be that the computer-controlled functions were

[832] Michael Meier, 'Lethal Autonomous Weapons Systems - Is It the End of the World as We Know It... Or Will We Be Just Fine' in Winston Williams and Christopher Ford (eds), *Complex Battlespaces the Law of Armed Conflict and the Dynamics of Modern Warfare* (Oxford University Press, 2019) 328.
[833] Marco Sassòli, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare* (Edward Elgar, 2019) 528.

legally regulated. A second would be that the control exercised by the system over those functions and, as such, by its programmers, would be such that its human operator could not reasonably be considered to have effective control. Otherwise put, the individual responsible for 'pulling the trigger' and discharging the weapon would no longer have sole responsibility for the decision to engage. In this case, an element of effective human control over the AWS would be coded into the system during its development, rather than being exercised at the point of its deployment or discharge. Typically, such development would be completed before the outbreak of any armed conflict within which the weapon was deployed.[834]

Next, it is important to consider whether these circumstances have yet been seen, or whether publicly available development plans indicate future circumstances such as these. Current weapon systems do not have a level of autonomous capability that would raise any serious concerns about programmer responsibility. Nevertheless, many of the component technologies that would be required for such systems are already in development or existence. The level of autonomy that would be required to raise such concerns may be low, given accessorial modes of liability. If other conditions of criminal liability are met, weapon programmers may well have enough control over prescribed AWS acts to be held accountable for any resulting crimes. What is important here, is that the other conditions of criminal liability must also be met. In the following sections, this dissertation will examine some of the requisite threshold elements for criminal liability in terms of AWS. In particular, it will discuss those which are relevant to the matter of programmer liability.

Armed Conflict as a Threshold Requirement

Evidently, for a war crime to occur, the offending act must be committed during a period of armed conflict; IHL only applies in such cases. In the case of war crimes trials, it is clear that many charges relate to the performance of specific acts during the course of an armed conflict. In others, prosecutions are challenged to prove that the alleged crimes were, indeed, committed during an armed conflict.[835] The official design of this threshold requirement, continually referenced by national and international criminal courts and tribunals, was detailed by the ICTY Appeals Chamber during its first trial against Duško Tadić:

[834] Christopher Ford, 'Autonomous Weapons and International Law' (2017) 69 *The South Carolina Law Review* 463.
[835] Gary Solis, *The Law of Armed Conflict: International Humanitarian Law in War* (Cambridge University Press, 2016) 545.

'An armed conflict exists whenever there is a resort to armed force between states or protracted armed violence between governmental authorities and organized armed groups or between such groups within a state. [IHL] applies from the initiation of such armed conflicts and extends beyond the cessation of hostilities until a general conclusion of peace is reached; or, in the case of internal conflicts, a peaceful settlement is achieved. Until that moment, [IHL] continues to apply …'[836]

This decision, in accordance with treaty and customary international law, differentiates between international and non-international armed conflicts and provides an alternative threshold test for each of these, giving the latter a much higher threshold. International criminal trials often commit notable resources to proving or disproving the armed forces context and, if it does, to establishing whether this conflict is international or non-international. For any war crimes under the Rome Statute, prosecutors must prove the context of either an international or non-international armed conflict.[837]

In terms of programmer liability, the biggest issue is that most development work occurs beyond the context of any armed conflict. Development typically takes place in peace time and in a commercial context, led by a corporate or government entity. Indeed, this could be the result of greater academic research by university researchers.

It is feasible that, during an enduring armed conflict, weapon system development and deployment could take place during the course of a conflict. Given that AWS have long lead times, this scenario, albeit possible (US forces have been present in Afghanistan for over 18 years), will be unusual. Therefore, in extreme circumstances, should other threshold requirements be met, programmers may be at risk of prosecution for war crimes. What is more likely, however, is that AWS development will be complete long before the system is deployed in an armed conflict and, indeed, before that armed conflict commences. As such, it is important to consider whether the

[836] *Prosecutor v Tadić* (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction) (International Criminal Tribunal for the Former Yugoslavia, Appeals Chamber, Case No IT-94-1, 2 October 1995) [70].
[837] Sasha Radin and Jason Coats, 'Autonomous Weapon Systems and the Threshold of Non-International Armed Conflict' (2016) 30 *Temple International and Comparative Law Journal* 133.

temporal distance between an armed conflict and an AWS' prior development activity will prevent programmers from being held to account for AWS crimes.

According to the Elements of Crimes, the classification of a war crime requires that the alleged conduct 'took place in the context of and was associated with an [international or non-international, depending upon the precise provision of the Statute,] armed conflict.'[838] *Prima facie*, any action performed before the onset of an armed conflict will not pass the 'context of' test and, as such, cannot be considered war crime. This is true, irrespective of the fact that prior AWS development for armed conflicts would most likely pass the 'associated with' test.[839]

Arguably, programmer activity is limited to the development phase. However, if the operator cannot later modify this work, it may be better placed at the point where the AWS' pre-programmed behaviour manifests during a conflict. Although this element of AWS development may support the idea of programmer liability, it does not circumvent the IHL's contextual threshold requirement. At most, it supports the notion of programmers being held accountable by any body of law that applies during the development phase. Such law could include product liability rules, as outlined by the programmer's domestic laws.

Principal and Accessorial Liability

As well as proving the fundamental elements of a given charge, prosecutors must also refer to Article 25 of the Rome Statute and prove criminal liability on the basis of the grounds for individual criminal responsibility listed therein. As such, the nature of an AWS' development is significant and has a number of noteworthy implications.

Importantly, weapon system development defines the behaviour of a system but does not involve the military application of that system (this is performed by the operator). Accordingly, even if a programmer had a significant level of control over an AWS' proscribed act and had the requisite

[838] International Criminal Court, Elements of Crimes, Doc No ICC-ASP/1/3 and Corr.1 and RC/11 (adopted 11 June 2010).
[839] Knut Dörmann, 'Preparatory Commission for the International Criminal Court: The Elements of War Crimes' (2000) 82 *International Review of the Red Cross* 771.

intent, their actions would still be performed by another organisation or individual.[840] Weapon development, alone, represents the preparation behind a proscribed act and not its physical performance. As such, it is unlikely that weapon systems programmers could be charged as physical perpetrators of any war crime, as defined by Article 25(3)(a). The only exception would be if a programmer were proven to have had sufficient control over an AWS that they could commit an offense 'through another person, regardless of whether that other person is criminally responsible.' This second individual would be the operator who deployed the weapon system. In some cases, this deployment could take place years after the system's development.[841]

It is worth considering another scenario which applies equally to conventional weapons and weapons of mass destruction; if there is evidence of a clear common criminal purpose and weapon programmers create a weapon system for a pre-determined, illegal purpose, prosecutors will still be able to hold programmers to account, despite their development actions having been conducted before the onset of the armed conflict. Although these circumstances would be incredibly rare, there are a number of political regimes that have already been seen to use whichever resources they can access. The international community has witnessed such regimes using technical and scientific expertise to develop new capabilities and subsequently use these capabilities, sometimes against their own citizens. It is clear that common criminal purpose doctrine covers preparatory acts that deliberately contribute to criminal activity.[842]

Further, while AWS programmers are said to have some level of control over system actions, they exercise this control through the system software and any other subsystems that they design. The extent of this control depends on the system's level of autonomy when performing a given action. With this autonomy determining the relationship between an AWS and its operator, and increased autonomy preventing the operator from intervening or exercising direct control over proscribed acts, it will also determine the ability for prosecutors to hold programmers to account for system

[840] Jarna Petman, 'Autonomous Weapons Systems and International Humanitarian Law: Out of the Loop?' (2017) Research Reports, Erik Castrén Institute of International Law and Human Rights, Helsinki 46.
[841] Liron Shilo, 'When Turing Met Grotius AI, Indeterminism, and Responsibility' (9 April 2018). Available at SSRN: <https://ssrn.com/abstract=3280393> accessed 27 February 2020 35.
[842] Rome Statute of the International Criminal Court, opened for signature 17 July 1998, 2187 UNTS 90 (entered into force 1 July 2002) Rome Statute art 25(3)(d).

actions. The level of autonomy is, therefore, the most likely means by which liability can be determined.[843]

As previously discussed, AWS autonomy determines the levels of control and responsibility shared by system operators and programmers. Provided an operator still has significant control over the weapon system's functions, the programmer and operator will share its control. It appears that operators will always, at least, be able to stipulate the time and place of activation. It is possible, however, that in specific circumstances, future system programmers may have effective control over system actions. As such, this control may render soldiers and commanders unable to control the AWS, unable to intervene, and unable to be held accountable for the instigation of its actions. It is thus necessary to consider two modes of liability. The first is that by which a programmer contributes to, but does not directly control, the instigation and delivery of a course of action and by which military operators cannot meaningfully influence this course of action.[844] In cases where programmers and operators have some level of shared control over an AWS, the most appropriate and likely ground for liability would be that they were, pursuant to Article 25(3)(c), an accessory who 'aids, abets or otherwise assists in [the] commission [of the crime] … including providing the means for its commission.'

Ex Ante Aiding and Abetting: International Legal Theory

Both grounds for criminal liability would need the criminal conduct to take place within the context of, and be associated to, an armed conflict. Should an AWS be deployed during the course of an armed conflict and commit a serious legal offence, the context of the conduct is somewhat clear. The key issue is whether preparatory acts, later completed through another person or designed to aid, abet or assist the commission of a crime, can be occur before the outbreak of a conflict.

International war crimes trials have provided no theoretical support for the debate on individual criminal responsibility when the individual's associated actions precede the armed conflict. Some

[843] Marcus Schulzke, 'Autonomous Weapons and Distributed Responsibility' (2013) 26 *Philosophy and Technology* 213.
[844] Stuart Maslen, 'Autonomous Weapons Systems and International Criminal Law' in Stuart Maslen, Nathalie Weizmann, Maziar Homayounnejad, & Hilary Stauffer (eds), *Drones and Other Unmanned Weapons Systems under International Law* (Brill, 2018) 245.

general statements have been made on potential accessorial liability for related acts that take place before the crime itself. The ICTY Appeals Chamber in the *Blaškić* judgment affirmed via *obiter dicta* that '[T]he *actus reus* of aiding and abetting a crime may occur before, during, or after the principal crime has been perpetrated, and that the location at which the *actus reus* takes place may be removed from the location of the principal crime.'[845] This statement was, however, one of mere principle and was not tested by the facts of that trial. Indeed, the trial decided that aiding and abetting did not offer suitable grounds for criminal liability. Nevertheless, the allegations made in this trial did not refer to preparatory acts completed before the outbreak of hostilities in Bosnia-Herzegovina.

In the judgement against Charles Taylor, The Trial Chamber of the Special Court for Sierra Leone acknowledged the statement of principle made by the ICTY Appeals Chamber in *Blaškić*:

'The Accused may aid and abet at one or more of the planning, preparation or execution stages of the crime or underlying offence. The lending of practical assistance, encouragement or moral support may occur before, during or after the crime or underlying offence occurs. The actus reus of aiding and abetting does not require specific direction. No evidence of a plan or agreement between the aider and abettor and the perpetrator is required, except in cases of ex post facto aiding and abetting where at the time of planning or execution of the crime, a prior agreement exists between the principal and the person who subsequently aids and abets the principal.'[846]

Once again, the chamber considered *ex ante* acts that would amount to aiding and abetting but, unlike in *Blaškić*, this ground for individual criminal liability led to a conviction. Contrasting the hypothetical case in which a weapon programmer completes their related acts before the onset of a conflict, Taylor was found guilty of aiding and abetting during the course of the conflict in Sierra Leone. Importantly, the chamber considered that in terms of the alleged crimes, his continued supply of troops, arms, ammunition, encouragement, operational support and moral support to the RUF/AFRC forces all represented significant contributions.

[845] *Prosecutor v Blaškić (Appeal Judgement)* (International Criminal Tribunal for the Former Yugoslavia, Appeals Chamber, Case No IT-95-14-A, 29 July 2004) [48].
[846] *Prosecutor v Taylor* (Judgement) (Special Court for Sierra Leone, Trial Chamber II, Case No SCSL03-01-T, 18 May 2012) [484].

Without any legal theory to support true *ex ante* conduct, it is difficult to forecast the potential decisions of a court. Given that the Elements of Crime require the context of an armed conflict, Article 22(2) of the Rome Statute stipulates that 'the definition of a crime shall be strictly construed and shall not be extended by analogy', and that 'in case of ambiguity, the definition shall be interpreted in favour of the person being investigated, prosecuted or convicted,' it is likely that any ICC chamber called upon for such matters will interpret the requisite elements quite literally.

The Application of the Effective Control Test within the Robotic Context

On face value, it appears that the programmers who are employed by a government agency have sufficient control over AWS. This is important given the fact that the programmer is ultimately responsible for issuing the instructions that guide the machine. For example, programmers develop the software that AWS use to learn from new data sets.[847] When AWS receive an order from a programmer in the form of input, the software upon which the system operates instructs the robot to perform a given function. As the software governs what assignments a robot executes and in what way, the programmer ultimately instructs the AWS, both on and off the frontline.

In line with international obligations, states will limit deployment of AWS to the robots that are in full adherence with IHL.[848] Programmers will develop software applications that fully incorporate IHL requirements as a means of facilitating weapon systems to produce suitable solutions. In effect, through the software that is designed and implemented, programmers possess the ability to preclude AWS from engaging in actions that cannot be justified. In this regard, programmers possess a degree of power that is comparable to that of a military leader. Specifically, military superiors instigate certain actions to avert the commission of crimes.[849] For example, military commanders are responsible for ensuring subordinates act within the realms of IHL practices and

[847] Delegation of Italy, Towards a Working Definition of AWS, Statement by the Delegation of Italy to the Conference on Disarmament, CCW 2016 Informal Meeting of Experts on AWS (Apr. 11-15, 2016), https://www.unog.ch/80256EDD006B8954/(httpAssets)/06A06080E6633257CI257F9B002BA3B9/$file/2016_LAWSMX_towardsaworkingdefinition_statementsItaly.pdf.

[848] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 85(3)(a), Jun. 8, 1977, 1125 U.N.T.S. 3; Rome Statute of the International Criminal Court art. 8(2)(b)(i) and art. 8(2)(e)(i), Jul. 17, 1998, 2187 U.N.T.S. 90, (this is the case for both international and non-international armed conflicts).

[849] *Prosecutor v. Halilovic (Trial Judgment)* (International Criminal Tribunal for the former Yugoslavia, Trial Chamber, Case No IT-01-48-T, 16 November 2005) [96].

for reprimanding those that fail to do so.[850] A programmer who develops and implements code to ensure that AWS perform to the required standard is analogous to a military leader who performs actions that are designed to maintain order among subordinates.[851] Supervisors deter subordinates from committing crimes by threatening reprimand. Programmers develop software modules with the objective of preventing AWS from acting in a way that contravenes IHL. By creating an application that allows AWS to learn through its interactions with the external environment, the programmer can be perceived to occupy a position that is comparable to that of a military commander who ensures his or her subordinates act within the realms of IHL.[852] A further parallel that can be drawn between the roles of programmers and military leaders is that both an AWS and a soldier can act in an unpredictable manner. In fact, soldiers can actively choose to disobey orders that are issued from above.

However, a closer examination highlights how the design of AWS does not indicate that a programmer has effective control over AWS. Gary Marchant et al. argued:

'Now, programs with millions of lines of code are written by teams of programmers, none of whom knows the entire program; hence, no individual can predict the effect of a given command with absolute certainty, since portions of large programs may interact in unexpected, untested ways.'[853]

As artificial intelligence applications are inherently complex, there is a lack of clarity as to whether a programmer can be trained to have responsibility for reviewing the full content of the program. According to a data scientist named Cathy O'Neil, programmers do not understand the algorithms they develop, nor can they interpret them.[854] While programmers have the ability to chart the forms

[850] *Prosecutor v. Naser Oric (Trial Judgment)* (International Criminal Tribunal for the former Yugoslavia, Trial Chamber, Case No IT-03-68-T, 30 June 2006) [294].
[851] *Prosecutor v. Naser Oric (Trial Judgment)* (International Criminal Tribunal for the former Yugoslavia, Trial Chamber, Case No IT-03-68-T, 30 June 2006) [294].
[852] Delegation of Italy, Towards a Working Definition of AWS, Statement by the Delegation of Italy to the Conference on Disarmament, CCW 2016 Informal Meeting of Experts on AWS (Apr. 11-15, 2016), https://www.unog.ch/80256EDD006B8954/(httpAssets)/06A06080E6633257CI257F9B002BA3B9/$file/2016_LAWSMX_towardsaworkingdefinition_statementsItaly.pdf.
[853] Gary Merchant et al., 'International Governance of Autonomous Military Robots' (2011) 12 *Columbia Science and Technology Law Review* 284.
[854] Downloading Decision: Could Machines Make Better Decisions For Us? CBC RADIO (Jul. 12, 2017), http://www.cbc.ca/radio/ideas/downloading-decision-could-machines-make-better-decisions-forus-1.3995678.

of code that a software package uses and the way in which the various modules interact, possessing an overview of the way in which the system operates does not correspond with the way in which the system performs in a given situation.[855]

In light of the fact that every programmer has a different influence on the architecture of AWS, individual programmers cannot be fundamentally aware of the way in which the various elements of code interact with each other.[856] It can be very challenging to pinpoint an individual programmer as the software architect. This challenge is embodied in the exploration of the effective control test, which wasn't intended to address situations of this nature; i.e., situations in which several different people are involved in the directions provided to a subordinate. This point was highlighted in the case of *Prosecutor v. Nahimana*,[857] in which the International Criminal Tribunal for Rwanda (ICTR) found that membership of a collegiate group, such as a board of directors, does not sufficiently represent the presence of effective control.[858] An individual can only be considered to be a superior if she or he 'had the power to take necessary and reasonable measures to prevent the commission of the crime.'[859] This point was extended by the ICTY Trial Chamber in *Prosecutor v. Oric,* which ruled that a fundamental consideration in determining effective control pertains to the extent to which the accused had 'the ability to maintain or enforce compliance of others with certain rules and orders.'[860] It is uncertain as to whether a sole programmer can be found to satisfy the *Nahimana* and *Oric* criteria. A program operates in accordance with how its various components interact.[861] Even in a situation in which a programmer has coded a significant aspect of the software, his or her ability to preclude an AWS from executing a war crime is purely theoretical.

---

[855] Tom Keeley, 'Auditable Policies for Autonomous Systems' Paul Sharre & Andrew Williams (eds), *Autonomous Systems: Issues for Defence Policymakers* (Nato, 2015) 221.
[856] Gary Merchant et al., 'International Governance of Autonomous Military Robots' (2011) 12 *Columbia Science and Technology Law Review* 284.
[857] *The Prosecutor v. Ferdinand Nahimana, Jean-Bosco Barayagwiza, Hassan Ngeze (Appeal Judgment)* (International Criminal Tribunal for Rwanda, Appeals Chamber, Case No ICTR-99-52-A, 28 November 2007).
[858] *The Prosecutor v. Ferdinand Nahimana, Jean-Bosco Barayagwiza, Hassan Ngeze (Appeal Judgment)* (International Criminal Tribunal for Rwanda, Appeals Chamber, Case No ICTR-99-52-A, 28 November 2007) [788].
[859] *The Prosecutor v. Ferdinand Nahimana, Jean-Bosco Barayagwiza, Hassan Ngeze (Appeal Judgment)* (International Criminal Tribunal for Rwanda, Appeals Chamber, Case No ICTR-99-52-A, 28 November 2007) [788].
[860] *Prosecutor v. Naser Oric (Trial Judgment)* (International Criminal Tribunal for the former Yugoslavia, Trial Chamber, Case No IT-03-68-T, 30 June 2006) [294].
[861] Gary Merchant et al., 'International Governance of Autonomous Military Robots' (2011) 12 *Columbia Science and Technology Law Review* 284.

While the performance of AWS varies according the complexity of the model and the datasets on which it is based, the continually embryonic nature of the software means that it is very difficult for a programmer to take action and modify the underlying architecture of the robot once it is in operation on the front line.[862] The tools that are currently available don't enable the programmer to ascertain what power the machine will allocate to neural connections in a given situation or the way in which it will arrange the symbols associated with a genetic algorithm when attempting to solve a problem.[863] This adds to the programmer's absence of understanding about the operation of the software.[864] The programmer has no means of predicting the outcomes of the decisions made by the robot.[865] The very nature of AI software acts as a limitation that prevents the programmer being forewarned about the execution of the code on the frontline.

A further challenge associated with allocating effective control to a programmer who was responsible for developing an element of the program concerns the way in which the programming team is structured. There is typically a team leader in place who is responsible for managing several developers and approving the program.[866] As such, individual programmers who are responsible for developing elements of the software are not likely to have supervisory authority. In absence of this authority, the programmer should not be held accountable for any war crimes that are the result of the actions of AWS because he or she does not have the ability to manage the work of the other programmers and take appropriate action to ensure that the software runs purely in accordance with the intended outcomes.

---

[862] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Penguin Random House, 2016) 24; William Wallach, Predictability and Lethal Autonomous Weapons Systems (LAWS), IEET (16 April 2016), <https://ieet.org/index.php/IEET2/print/11873> accessed 27 February 2020; Andreas Matthias, 'The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata (2014) 6 *Ethics and Information Technology* 175.

[863] Andreas Matthias, 'The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata (2014) 6 *Ethics and Information Technology* 176.

[864] Michael Fisher et al., 'Verifying Autonomous Systems: Exploring Autonomous Systems and the Agents That Control Them' (2013) 56 *Communications of the ACM* 84.

[865] Michael Fisher et al., 'Verifying Autonomous Systems: Exploring Autonomous Systems and the Agents That Control Them' (2013) 56 *Communications of the ACM* 84.

[866] Marilyn Mantei, 'The Effect of Programming Team Structures on Programming Tasks' (2011) 24 *Communications of the ACM* 106.

It is worth asking, therefore, whether someone who holds responsibility for overseeing the outputs of a team of programmers and ultimately signing off the code has effective control over the AWS, even when it is on use on the frontline. This objective determination varies according to the type of control the lead programmer has over the code and is comparable to the nature of control a military superior has over his or her subordinates. The lines of code and the subordinates are analogous to some extent. A group of subordinates could join forces to commit a crime. In the AWS context, the interaction between the lines of code and the way in which they are executed could lead to a machine sparking an international crime. The ICTY Trial Chamber in *Prosecutor v. Oric* highlighted how the attribution of accountability is determined by the extent to which the superior had the means to prevent the crimes being commissioned as opposed to his or her familiarity with the perpetrators.[867] The head programmer has the ability to ensure that unsuitable software components are not included in the program. *Prosecutor v. Oric* found that it was irrelevant that the head programmer was not aware of the final architecture the AWS assimilated on the frontline. Moreover, according to the ruling of *Prosecutor v. Oric*, to possess effective control, the head programmer is not required to be familiar will all aspects of the software and the way in which they interact with one another.[868] The head programmer's power to eliminate unacceptable software modules, approve the outline of AWS and supervise the outputs of individual programmers is enough to represent effective control.

However, this line of inquiry is deficient. It is precipitate to assign effective control to a head programmer on account of the fact that he or she has the ability to verify the code and instruct the team members to change the software. Arguably, the test of effective control assumes that that the superior is in a position to screen the intents, discussions or behaviour of his or her subordinates. This was made clear in the decision of the ICTY Trial Chamber in *Prosecutor v. Blaskic*. The Judges ruled that an individual has the potential to preclude crimes from being commissioned in situations in which he or she is required to submit formal reports to the relevant authorities as a means of enabling them to take suitable measures.[869] To have the knowledge and insight required

[867] *Prosecutor v. Naser Oric (Trial Judgment)* (International Criminal Tribunal for the former Yugoslavia, Trial Chamber, Case No IT-03-68-T, 30 June 2006) [294].
[868] *Prosecutor v. Naser Oric (Trial Judgment)* (International Criminal Tribunal for the former Yugoslavia, Trial Chamber, Case No IT-03-68-T, 30 June 2006) [294].
[869] *Prosecutor v. Tihomir Blaskic (Appeal Judgement),* (International Criminal Tribunal for the former Yugoslavia, Appeals Chamber, Case No IT-95-14/A, 29 July 2004) [69].

to formulate and submit reports, a superior needs to oversee the behaviour of his or her subordinates. It is only through scrutinising subordinates' conduct and conversations that the superior can identify their intentions and, as such, become aware that a subordinate intends to commit a crime. In the same way, there would be a requirement for the head programmer to monitor the evolution of the AWS architecture as it is in operation on the frontline as it is only through doing so that he or she could access advanced notice that the software may be performing in an unanticipated way.

Some studies have found that it could be possible to oversee a machine's learning process.[870] For example, programmers could implement a function that mandates information is displayed in such a way—for example, a decision tree—that the machine can effectively report the factors it took into consideration when making its decision.[871] Each branch on the decision tree would represent an alternative course of action, while the leaves could represent the contributory aspects that had an influence on the decision.[872] However, one problem with this approach is that mechanisms of this nature do not allow the head programmer to recognize the way in which the software has changed once it is in operation on the frontline. The software will evolve in response to the situations it encounters on the battlefield.[873] The head programmer will not have the ability to monitor all weapons systems that have been produced by the company. In the absence of knowledge about the way in which the software has evolved during use, the head programmer is not in a position to know that an unanticipated interaction or malfunction is imminent. Due to the fact that having the ability to become aware of the risk of improper conduct is fundamental to the concept of effective control, the head programmer may not have the material ability to inhibit the robot from acting in a way that represents an international crime.

---

[870] Peter Margulies, 'The Other Side of Autonomous Weapons: Using Artificial Intelligence to Enhance IHL Compliance' in Ronald Alcala and Eric Talbot Jensen (eds), *The Impact of Emerging Technologies on the Law of Armed Conflict* (Oxford University Press, 2018) 156.

[871] Peter Margulies, 'The Other Side of Autonomous Weapons: Using Artificial Intelligence to Enhance IHL Compliance' in Ronald Alcala and Eric Talbot Jensen (eds), *The Impact of Emerging Technologies on the Law of Armed Conflict* (Oxford University Press, 2018) 156.

[872] *Decision Tree*, Investopedia, http://www.investopedia.com/terms/d/decision-tree.asp (last visited May 4, 2019); Stuart Russell and Peter Norvig, *Artificial Intelligence A Modern Approach* (Pearson, 2010) 757.

[873] William Wallach, Predictability and Lethal Autonomous Weapons Systems (LAWS), IEET (16 April 2016), <https://ieet.org/index.php/IEET2/print/11873> accessed 27 February 2020.

Many scholars have argued that the inherent complexity of robots that possess artificial intelligence entails that it is not possible for a sole person, like a lead programmer, to have a working comprehension of how the various elements of the software interact.[874] As no one person can comprehend how the software components interact with one another, it is doubtful as to whether a single person has the ability to possess complete knowledge of the operation of the software.[875] Because possessing the ability to become aware of the risk of inappropriate conduct is fundamental to the concept of effective control, it is arguable that the head programmer lacks the material ability to inhibit the robot from performing actions that represent international crime.

A counterargument to this theory could be that there is no need for the head programmer to be aware of how the various mechanisms of the code function when an AWS is operating on the frontline. Typically, the individuals who occupy a position high in the chain of command, such as generals and heads of state, are ultimately responsible for the behaviour of the subordinates who operate low in the chain of command, even if such superiors are not in proximity to those who committed war crimes and may not have possessed knowledge of how the subordinates interacted.[876] However, a head programmer is not in the same position as a general. The principle of command responsibility attributes accountability to those people who operate at a high level of command according to the notion that they control subordinates via a chain of command through which they are required to ensure compliance with IHL through the implementation of appropriate measures; for example, regular reports.[877] The chain of command that can be observed in military factions is specifically designed to prevent defiance and is bolstered by the imposition of criminal sanctions on those who do not maintain sufficient oversight of the behaviours of their subordinates.[878] In contrast, by their very nature, artificial intelligence programs are conducive to

[874] Gary Merchant et al., 'International Governance of Autonomous Military Robots' (2011) 12 *Columbia Science and Technology Law Review* 284; William Boothby, 'Highly Automated and Autonomous Technologies' in William Boothby (eds), *New Technologies and the Law in War and Peace* (Cambridge University Press, 2018) 154.
[875] William Boothby, 'Highly Automated and Autonomous Technologies' in William Boothby (eds), *New Technologies and the Law in War and Peace* (Cambridge University Press, 2018) 155.
[876] *Prosecutor v. Mengistu et al*., S.P.O Investigation File No. 401/85, Reply Submitted in Response to the Objection Filed by Counsels for Defendants, T 1(6) (Ethiopian Special Prosecutor's Office, May 23, 1995).
[877] Report of the International Commission of Inquiry on Darfur to the U.N. Secretary General, 558 (25 January 2005); *Prosecutor v. Tihomir Blaskic (Appeal Judgement)*, (International Criminal Tribunal for the former Yugoslavia, Appeals Chamber, Case No IT-95-14/A, 29 July 2004) [69].
[878] National Defense and the Canadian Armed Forces, *Chapter 1: The Purpose of Military Justice*, Government of Canada (2017), available at <www.forces.gc.ca/en/about-reports-pubs-military-law-summary-trial-level/ch-1-purpose-of-mil-justice.page> accessed 28 February 2020.

a robot acting in an unforeseen way. Individual programmers do not have effective control over AWS when they are operating on the frontline because there is no chain of command by which the lead programmer can be linked with the system. There is a requirement for a superior to have effective control over a subordinate for him or her to have effective control. Furthermore, the subordinate should, in turn, have effective control over the people operating below him or her.[879] When a subordinate who is responsible for monitoring the conduct of AWS does not have effective control over it, the head programmer also lacks effective control. As such, it is reasonable to conclude that a lead programmer does not have effective control over AWS when it is operational on the frontline.

A further hurdle prevents a lead programmer from establishing effective control. For effective control to exist, the superior needs to have the required degree of control over the subordinate at the time at which a crime is commissioned.[880] Meloni elucidated on the rationale that underpins this requirement. The individual who fails to control the subordinates and, thereby, creates a risk that crimes will be committed is not a different individual the person who does not act in a reasonable fashion and take the required measures to avert the risk from occurring. Meloni's reasoning is substantiated by the fact that the likelihood of imposing sanctions for disobedience is closely correlated with an individual's capacity to regulate the behaviour of subordinates.[881]

However, there is a lack of clarity as to the extent to which a lead programmer will have a chance to frequently monitor the performance of an application after it has been transferred to the armed forces. By virtue of its nature, the software architecture that supports AWS is embryonic.[882] As such, this architecture needs to be monitored on a regular basis. Even in situations in which a lead programmer has effective control over the subordinates within the armed forces who are tasked with monitoring the operation of the robot on the frontline and reporting all findings accordingly, due to the very nature of an AWS, subordinates will not be in a position to predict what decisions

[879] Report of the International Commission of Inquiry on Darfur to the U.N. Secretary General, 558 (25 January 2005).
[880] *Prosecutor v. Zdravko Mucic aka "Pavo", Hazim Delic, Esad Landzo aka "Zenga", Zejnil Delalic (Appeal Judgement)*, (International Criminal Tribunal for the former Yugoslavia, Appeals Chamber, Case No IT-96-21-A, 20 February 2001) [306].
[881] Chantal Meloni, *Command Responsibility in International Criminal Law* (T.M.C. Asser Press, 2010) 3.
[882] William Wallach, Predictability and Lethal Autonomous Weapons Systems (LAWS), IEET (16 April 2016), <https://ieet.org/index.php/IEET2/print/11873> accessed 28 February 2020.

it will make when it is operating in a battlefield. The subordinates involved will often be unable to receive advanced notice of any imminent danger that the robot is going to take unwarrantable action. In situations in which the recording boxes involved don't provide a complete view of the neural network and the process by which AWS make each decision, the subordinate does not have effective control over AWS. If the subordinates do not have effective control over the AWS, neither does the lead programmer. On the contrary, if subordinates have access to the tools required to monitor operations and learn the process by which the AWS solves problems, they may be perceived to have effective control over the AWS. In this case, if it is established that the lead programmer possesses effective control over the subordinates, he or she can also be held accountable.

A further question that is of interest concerns the extent to which the lead programmer possesses the material capacity to prevent AWS from instigating a war crime having tested the way it performs in virtual frontline scenarios. This notion is problematic due to the fact that it is based on the broad assumption that it is possible to exhaustively test the interactions that take place between software components and the decisions that the AWS will make during warfare. Robots that possess artificial intelligence are 'complex adaptive systems' that can adjust their actions in a major way after confronting a 'tipping point' incident.[883] On this basis, it is very cost prohibitive, if even possible, to test them. The concept that it may not be possible to fully test robots is also reinforced by the detail that people are not capable of foreseeing every situation a robot or solider may confront on the frontline.[884] Soldiers operate under general commands, such as to open fire in response to an 'imminent threat' to their life; however, they are not issued with very specific guidance on the way in which they should respond to a very specific set of circumstances because the battlefield is volatile.[885] As it is not possible to predict every situation a soldier will confront, it is also not possible for the AWS to be exposed to all potential frontline situations in a virtual environment. On this basis, programmers are not able to systematically test AWS.

[883] Jai Galliott and Tim McFarland, 'Autonomous Systems in a Military Context (Part 1): A Survey of the Legal Issues' (2016) *International Journal of Robotics Applications and Technologies* 42.
[884] Jai Galliott and Tim McFarland, 'Autonomous Systems in a Military Context (Part 2): A Survey of the Legal Issues' (2016) *International Journal of Robotics Applications and Technologies* 62.
[885] Patrick Lin, George Bekey, and Keith Abney, 'Autonomous Military Robotics: Risk, Ethics, and Design' (2008) California Polytechnic State University San Luis Obispo 78.

While the lead programmer should aim to develop reliable machines, due to the way in which artificial intelligence functions, it is conducive to an AWS acting in an unanticipated manner. Each time a robot assimilates a new task, its underlying algorithm self-modifies to ensure that the behaviour of the robot changes in the future.[886] These changes accumulate over time. It is entirely possible that the accumulative changes will eventually result in a major reorganization of the structure of the software. It is challenging to conceive how a lead programmer who is unable to anticipate the way in which the AWS will modify its algorithm after being exposed to a new situation on the frontline can be held to have a material ability to avert the commission of crimes. Of course, it is feasible that this state of affairs may change over time as a result of the development of technology. If it can become possible to monitor and record the internal operation of the software, a lead programmer will meet more of the conditions of effective control. Depending on the way in which technology develops, it could potentially be possible to use the principle of command responsibility to hold state employees who are responsible for creating the architecture of a robot accountable if AWS behave in an unexpected way.

When it is not possible to establish that a lead developer or programmer has effective control over a robot, the individuals who are in a high position of command who allocated responsibility for developing the AWS lack effective control over the machine. The endgame is that the state officials from the Department of Defense who certify AWS could potentially be held responsible under the doctrine of command responsibility only in situations in which an individual programmer and lead programmer had proven effective control of the AWS during its operation on the frontline. On a practical level, the dynamic characteristics of artificial intelligence applications and the nature of applications that are employed to record the mechanisms of the neural network entail that it is very difficult to attribute effective control to any sole person within a state agency.[887]

The Requirement for Mens Rea

With aiding and abetting identified as the most likely ground for programmer liability, this section will consider the mental element requirement. Much like the physical element of an AWS-caused

[886] Alan Schuller, 'At the Crossroads of Control: The Intersection of Artificial Intelligence in Autonomous Weapon Systems with International Humanitarian Law' (2017) 8 *Harvard National Security Journal* 409.
[887] Ashley Deeks and Noam Lubell and Daragh Murray, 'Machine Learning, Artificial Intelligence, and the Use of Force by States' (2018) 10 *Journal of National Security Law and Policy* 26.

violation, the *ex ante* nature of a programmer's actions will also provide a significant challenge when prosecutors seek to identify the requisite mental element for criminal liability.

The ICTY Trial Chamber in *Anto Furundžija* provided some guidance on the requisite level of knowledge for aiding and abetting:

'[I]t is not necessary that the aider and abettor should know the precise crime that was intended and which in the event was committed. If he is aware that one of a number of crimes will probably be committed, and one of those crimes is in fact committed, he has intended to facilitate the commission of that crime, and is guilty as an aider and abettor.'[888]

Subsequently, the ICTY Appeals Chamber in *Blaškić* agreed with this statement,[889] suggesting that programmers could be found guilty of aiding and abetting without having known precisely how the AWS would be used. This could occur in cases whereby competent programmers program AWS behaviours that a reasonable person would consider to be criminal. To prove this liability, however, prosecutors would need to overcome two significant obstacles.

Firstly, present case law requires the accused to be aware of the physical perpetrator's criminal intent when they provide them with assistance. In the case of *Anto Furundžija*, the anti-terrorist unit had criminal intent and was conducting crimes while Furundžija was providing assistance. Equally, in the *Taylor* case, Taylor was aware of his soldiers' criminal intent and actions when he provided them with supplies. In the earlier post-WWII case *Zyklon B,*[890] German industrialists were found guilty of war crimes that violated Article 46 of the Hague Convention 1907, having known that their poison gas would be used to kill Allied nationals in concentration camps. In *Zyklon B,* it was determined that the physical perpetrators of the exterminations, the SS officers, had formed their intent when the gas was supplied to them. The industrialist suppliers were found

[888] *Prosecutor v Furundžija* (Judgement) (International Criminal Tribunal for the Former Yugoslavia, Trial Chamber, Case No IT-95-17/1-T, 10 December 1998) [246].
[889] *Blaškić* [50].
[890] 'Case No 9: The Zyklon B Case: Trial of Bruno Tesch and Two Others (British Military Court, Hamburg)' in United Nations War Crimes Commission, Law Reports of Trials of War Criminals (His Majesty's Stationery Office, 1947) vol 1, 93.

to have known this intent at the point of supply.[891] If the criminal intent of a perpetrator does not exist when a system programmer completes their work, existing legal theory does not hold that the programmer has the requisite mental state.[892]

Secondly, there is a specific mental element that relates to aiding and abetting. This is outlined in Article 25(3)(c) of the Rome Statute and supplements the general requirements of Article 30. It holds that a programmer's work would need to fulfil 'the purpose of facilitating the commission' of a crime. Not only would a prosecutor need to prove that the weapon programmer was aware of the criminal intent and that their own actions would support the crime, [893] but also that their actions were intended to support the crime, rather than simply to achieve a legitimate military objective or, indeed, to make a commercial profit.[894]

Prosecutors would also face the significant challenge of proving that the AWS programmer had committed a violation 'through another person, regardless of whether that other person is criminally responsible.' Although recent cases have suggested judicial disagreement,[895] the ICC has tended to use the 'control of the crime' approach when ruling on accusations of commission through third parties. Should this approach be followed, AWS programmers with criminal intent could produce weapon systems that act in a pre-determined way beyond the orders received from their operator. In these cases, however, the challenges are similar to those seen for aiding and abetting: the programmer's intended crime, or the crime which they can forecast, will take place at a later stage, during the course of an armed conflict. At the very least, prosecutors would be required to prove that the weapon system programmer was aware that the system would go on to act illegally. For instance, they would need to prove that the programmer knew the system was

[891] I.G. Farben Industrie A.G. for 'the use of poison gas, supplied by Farben, in the extermination of inmates of concentration camps' as a crime against humanity: '*Case No 57: The I G Farben Trial: Trial of Carl Krauch and Twenty-Two Others (United States Military Tribunal, Nuremberg)*' in United Nations War Crimes Commission, Law Reports of Trials of War Criminals (His Majesty's Stationery Office, 1949) vol 10, 5.
[892] Stuart Maslen, 'Autonomous Weapons Systems and International Criminal Law' in Stuart Maslen, Nathalie Weizmann, Maziar Homayounnejad, & Hilary Stauffer (eds), *Drones and Other Unmanned Weapons Systems under International Law* (Brill, 2018) 245.
[893] *Taylor* [487].
[894] Robert Cryer et al, *An Introduction to International Criminal Law and Procedure* (Cambridge University Press, 2010) 312.
[895] See, e.g., *Prosecutor v Chui* (Judgment Pursuant to Article 74 of the Statute) (International Criminal Court, Trial Chamber II, Case No ICC-01/04–02/12, 18 December 2012) [4]–[30] (Concurring Opinion of Judge Christine Van den Wyngaert).

unable to distinguish between combatants and non-combatants and would kill unidentified individuals. If a programmer was proven to have deliberately created an internal mechanism that could target a specific individual, known by them to be a protected non-combatant, this would clearly meet the *mens rea* requirements. Evidence of such deliberate acts would, however, be very rare.

Summary of Programmer Responsibility

It is likely that a programmer's involvement with an AWS will conclude before it is deployed within an armed conflict. This fact raises significant questions regarding the requisite elements of war crimes. First and foremost, there is a threshold requirement that any alleged attack occurs 'in the context of an armed conflict.' Consequently, weapon programmers may receive *de facto* immunity for any subsequent war crimes. Prosecutors may, however, claim that when a programmer's prior actions are realised 'in the [subsequent] context of an armed conflict', this satisfies the threshold requirement. This is, however, a novel argument, with no guarantee of support from legal decision makers. When considering aiding and abetting as a mode of liability, international legal theory does consider *ex ante* preparatory acts to be sufficient. Nevertheless, there is no current international legal theory to support the view that the aiding and abetting of war crimes can take place before an armed conflict begins.

AWS programmer liability is further hindered by the *mens rea* requirement for aiding and abetting. Any weapon programmer accused of aiding and abetting would have provided their services before the outset of an armed conflict. The criminal intent they are said to have supported, however, would have only emerged later, when the conflict was underway. If this temporal gap were to be bridged, current law would require significant amendment.

Even in cases where a prosecutor could establish the requisite elements, reference to the programmer may be very problematic in that it could misrepresent the way in which AWS are developed. Complex AWS will be developed by teams of people, across organisations. These individuals will collaborate on a wide network of subsystems, all with intricate interdependencies. In order to initiate a legal trial, prosecutors would need to identify the single individual who is

most responsible for any subsequent war crimes caused by the AWS; indeed, this may be too complicated.

These challenges suggest that, in order to better represent the new reality of weapon development the current normative framework should be developed. Provided the crime were committed in the relevant context, the threshold requirement for acts to take place 'in the context of an armed conflict' might be amended to explicitly or implicitly cover preparatory acts conducted before the start of the conflict. Potentially, the requirement for *mens rea* could also be clarified, covering aiding and abetting by programmers within the present context.

The Doctrine of Command Responsibility: A Poor Fit to Govern Artificial Intelligence Systems

Whenever the misuse of an AWS leads to a crime, superior responsibility could demonstrate the liability of its commanders. For instance, where an operational commander learns that one of their subordinates is using autonomous drones at the tactical level and conducting illegal attacks, the operational commander has a responsibility to prevent subsequent crimes and to discipline their subordinate (Geneva Convention API: Art. 86(2) and 87). Provided there is sufficient evidence to prove that the commander had effective control over criminal subordinates, their knowledge of the crimes and subsequent failure to prevent repercussion and punish the perpetrators would render them criminally liable. As detailed, rather than directly participating in a crime, superior responsibility imposes liability on account of commander's omissions, or failure to prevent repercussions and punish those responsible.

In order to assess the superior-subordinate relationship, the effective control test should remain the same when the key perpetrators of IHL violations use AWS for the commission of their crimes. Nevertheless, technological advances could mean that assessments of knowledge and reasonable prevention, as pillars of superior responsibility, need reassessment.

With regard to knowledge, military commanders whose troops operate AWS will find it difficult to persuade a court that they were unaware that their subordinates were operating such systems in an illegal manner. This should be the case even if the courts consider the 'had reason to know'

standard offered by the *ad-hoc* tribunals, or the ICC's standard of 'should have known'. Any state military or organised militia with sufficient resources to field AWS will also be able to continually monitor their use. Moreover, a competent commander would seek to exercise any observation methods possible in order to monitor the progress of their units' operations.[896] This real-time, continual monitoring ability should be a pre-requisite of any AWS and incorporated into the procurement process.[897]

Nevertheless, the fact that a commander has access to swathes of data will not necessarily mean that they are aware and should have been aware of their subordinates' actions. The mere fact that modern technologies can obtain increasing volumes of data and/or complicate the reality of the battlespace could, ultimately, contribute to the fog of war.[898] According to Cummings, 'command and control technology have outpaced human reasoning capabilities and traditional command structures.'[899] However, this should not be allowed to negate commanders' roles in ensuring LOAC compliance amongst their subordinates.[900] As such, there will be a requirement for new methods of data capture and analysis and interaction between human operators and systems, prioritising information about the actions, positioning and status of subordinate troops and the weaponry they are using, enabling commanders to continually monitor the use of AWS.[901]

The concept of superior responsibility implies a duty to prevent crime and to punish those who commit illegal acts. A duty to prevent crime commences as soon as a superior learns, or has reason

[896] For example, during multinational NATO operations, the Supreme Allied Commander for Europe (SACEUR) must '[e]stablish an intelligence architecture linking NATO Headquarters with national intelligence centres to provide the [Joint Force Commander] with a common, timely and accurate picture of the situation during all phases of the campaign' NATO. 2010. *AJP-01D Allied Joint Doctrine*, North Atlantic Treaty Organization, 21 December. Available online at <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33694/AJP01D.pdf> accessed 28 February 2020 par.0615(e).

[897] Kimberley Trapp, 'Great Resources Mean Great Responsibility: A Framework of Analysis for Assessing Compliance with API Obligations in the Information Age' in Dan Saxon (eds), *International Humanitarian Law and the Changing Technology of War* (Martinus Nijhoff/Brill, 2013) 156.

[898] Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (Cambridge University Press, 2010) 139.

[899] Mary Cummings, 'Automation and Accountability in Decision Support System Interface Design' (2006) MIT Human and Automation Laboratory. Available online at <http://web.mit.edu/aeroastro/labs/halab/papers/Cummings_JTS.pdf> accessed 28 February 2020 17.

[900] Claude Pilloud and Jean Pictet, 'Protocol I – Article 87 - Duty of Commanders' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) para 3560.

[901] Mary Cummings, 'Man Versus Machine or Man + Machine?' (2014) 29(5) *Intelligent Systems, IEEE* 62.

to discover, that a crime is planned, or being committed.[902] The duty to punish commences as soon as a superior learns that a crime has been committed.[903] As such, if the notion of superior responsibility is to remain relevant, there needs to be some level of interaction, even if not supervision, between a commander and the AWS under their command.

When AWS are used to effect illegal strikes, the scope of necessary and reasonable measures for the prevention of recurrences and punishment of perpetrators may vary. For example, military engagements using swarm technology will no doubt experience a comparatively higher tempo.[904] As the pace of combat increases, along with the pace of unlawful actions, commanders will become less able to prevent illegal conduct.

Yet, unlike human troops, many AWS can be deactivated.[905] As such, commanders' actions in terms of preventing or repressing illegality should also consider their actions in seeking to shut down the offending system. Part of their acquisition, including Article 36 legal reviews, should require AWS to have an override mechanism that superiors can use to stop their subordinates from misusing them, and to shut down, or assume control of, the system. By engaging these override mechanisms, commanders would demonstrate necessary and reasonable measures for the avoidance of further illegality. Conversely, a failure to engage these measures would amount to liability for the crimes.

Nonetheless, as outlined by Heyns, 'the power to override may in reality be limited because the decision-making processes of robots are often measured in nanoseconds and the information basis of those decisions may not be practically accessible to the supervisor. In such circumstances humans are *de facto* out of the loop.'[906] In these circumstances, a commander would still have a

[902] Article 28 of the Rome Statute, Articles 86 (2) and 87 of Additional Protocol I to the Geneva Conventions.
[903] Decision Pursuant to Art 61(7)(a) and (b) of the Rome Statute on the Charges of the Prosecutor against Jean-Pierre Bemba Gombo, *Bemba* (International Criminal Court, Pre-Trial Chamber II, Case No ICC-01/05-01/08-424, 15 June 2009) [437].
[904] Peter Fiddian, 'UAV Swarm Technology Trial Success' (*Armed Forces International News*, 13 March 2012). Available online at <http://www.armedforces-int.com/news/uav-swarm-technology-trial-success.html> accessed 28 February 2020.
[905] John Markoff, 'Old Trick Threatens New Weapons' (*The New York Times*, 26 October 2009). Available online at <http://www.nytimes.com/2009/10/27/science/27trojan.html?pagewanted=all&_r=0> accessed 28 February 2020.
[906] Christof Heyns, '*Report of the Special Rapporteur on Extra-Judicial, Summary or Arbitrary Executions'* (2013) A/HRC/24/47, 9 April, para 41.

duty to either override or shut down the autonomous system as soon as they were able, on identifying that it was being misused.

Matthias highlighted a general liability gap for machine-learning systems as, theoretically, manufacturers and operators cannot anticipate their future actions.[907] He notes that software programmers' influence over these machines reduces as they become more capable of developing according to their own experiences and environments; 'In a steady progression the programmer role changes from coder to creator of software organisms. In the same degree as the influence of the creator over the machine decreases, the influence of the operating environment increases.'[908] Nevertheless, it is probable that the challenges of control and predictability brought about by discretionary autonomy are understated, due to the possibility of emergent behaviour altering the result.

Behaviour of this sort could result from communications between an AWS's component parts or systems, or interactions between those systems and the circumstances surrounding its deployment. Considering the intricacies of the an AWS's programming, it is unlikely that humans could understand, let alone forecast, the outcomes of communication between its different programs. As such, it is likely that even a single AWS could be unpredictable, even when each of its component parts, independently, behaves in a predictable manner. Further, it has been proposed that AWS could operate in swarms, allowing complex behaviours to arise as the systems adhere to basic rules.[909] In these scenarios, even if a single AWS were entirely predictable and manageable, this would not be the case for the combined behaviour of a group of interacting systems. Moreover, the operating environment will influence an autonomous system. No two operating environments will be the same and, as such, AWS will behave in different manners in each, even if their coding remains the same. Ultimately, an autonomous system's actions are likely to be affected by the combination of all of these external factors, thus creating unique responsibility issues, posing challenges for the predictability and control of AWS.

---

[907] Andreas Matthias, 'The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata' (2004) *Ethics and Information Technology* 175.
[908] Andreas Matthias, 'The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata' (2004) *Ethics and Information Technology* 182.
[909] Peter Singer, *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century* (Penguin, 2009) 229.

An AWS's conduct will be limited by programmers at the research and development stage of its procurement. These limitations are likely to be both abstract and wide-ranging. Naturally, programmers will be able to transfer any liability to commanders, simply by acknowledging the systems' limitations.[910] Nonetheless, the behaviour of an AWS will also be influenced by the commander who, by choosing to engage with the system, will be required to add their own context-specific parameters.[911] This process transfers liability from the programmers to the commander as the programmers could then argue that they fulfilled their obligations when they set the system's initial limitations. As such, programmers could argue that any illegal actions carried out by the system are the product of the commander's work, or their failure to add specific limitations to the basic parameters, appropriate to the context in which the system is deployed.

Commanders could, however, argue the opposite, seeking to transfer liability to the system's programmers. As such, assessing a commander's responsibility is a complex task. The commander's actions follow those of the programmer. Therefore, the commander is only able to limit the system's behaviour insofar as the programmer's existing parameters will allow them to do so.[912] The commander's control over the AWS is thus limited, as is their ability to predict its behaviour. This could serve to justify that their individual responsibility for its actions is restricted. The context in which an AWS is intended for use will also limit the commander's burden of responsibility. Considered legally, and in accordance with the Rome Statute of the ICC, by replacing the direct human operator of a weapon system with an artificial alternative, the prerequisite superior–subordinate relationship could be agitated.[913] This is true because the relationship has, to date, been an interpersonal one.[914] Even if AWS were granted legal

[910] Robert Sparrow, 'Killer Robots' (2007) 24 *Journal of Applied Philosophy* 69.
[911] Geoffrey Corn, 'Autonomous Weapons Systems: Managing the Inevitability of Taking the Man Out of the Loop' in Nehal Bhuta, Susanne Beck, Robin Geiβ, Hin Liu, & Claus Kreβ (eds), *Autonomous Weapons Systems: Law, Ethics, Policy* (Cambridge University Press, 2016) 242.
[912] Alexander Bolt, 'The Use of Autonomous Weapons and the Role of the Legal Advisor' in Dan Saxon (eds), *International Humanitarian Law and the Changing Technology of War* (Martinus Nijhoff, 2013) 132.
[913] *Prosecutor v. Zdravko Mucic aka "Pavo", Hazim Delic, Esad Landzo aka "Zenga", Zejnil Delalic (Trial Judgement)*, (International Criminal Tribunal for the former Yugoslavia, Trial Chamber, Case No IT-96-21-T, 16 November 1998) [346]; *Prosecutor v. Halilovic (Appeal Judgment)* (International Criminal Tribunal for the former Yugoslavia, Appeals Chamber, Case No IT-01-48-A, 16 October 2007) [59]; Rome Statute of the International Criminal Court (Rome Statute), 1 July 2002, UN Doc. A/CONF.183/9.
[914] Guenael Mettraux, *The Law of Command Responsibility* (Oxford University Press, 2009) 156.

personhood, Article 25(1) only permits the ICC to rule over human beings. As a result, legally speaking, it would be impossible to impose the doctrine of command responsibility on an AWS, owing to the absence of a superior-subordinate relationship.

It could also be difficult to prove a commander's 'effective control' over an AWS as this requires them to have 'the power and ability to take effective steps to prevent and punish crimes which others have committed or are about to commit.' Considering the list of measures of effective control,[915] there will be notable issues in terms of disciplinary and investigatory powers and the ability to prevent AWS illegality. A commander's powers to influence, stop, or prevent an AWS's behaviour could be significantly limited by its architecture, rely upon the commander's own technical know-how and be impracticable, as machines cannot be punished in any meaningful way. Combined, these factors create significant challenges for confirming that a commander could control an AWS and have the requisite ability to dominate any such systems under their command. Circumstantial issues such as these could be avoided by increasing the onus placed upon the commander and requiring them to abort illegal missions or prevent such illegalities from occurring. Further, as AWS can increase the data-flow out of theatre, their employment could alter the criteria shaping the mental aspect of a crime. This results from communicational advances that risk overwhelming the commander, providing such vast quantities of information that they are unable to process it all.[916] Faced with this, Garraway believes that the 'should-have-known' standard would be better considered in terms of whether 'there was a degree of personal dereliction by the commander', thus keeping the task manageable.[917] Although this approach would balance the commander's abilities with their obligations, it greatly limits the content and parameters of their legal responsibilities. The command responsibility doctrine thus becomes insufficient, increasing the disconnect between the reliance upon it to overcome AWS impunity and its ability to attribute liability for their use.

[915] Guenael Mettraux, *The Law of Command Responsibility* (Oxford University Press, 2009) 164.
[916] Charles Garraway, 'The Application of Superior Responsibility in An Era of Unlimited Information' in Dan Saxon (eds), *International Humanitarian Law and the Changing Technology of War* (Martinus Nijhoff, 2013) 203.
[917] Charles Garraway, 'The Application of Superior Responsibility in An Era of Unlimited Information' in Dan Saxon (eds), *International Humanitarian Law and the Changing Technology of War* (Martinus Nijhoff, 2013) 203.

Another aspect of the mental consideration examines whether or not a commander is able to understand and rely upon the limitations put in place by the system's programmer. The answer to this question will have an impact on the commander's viable knowledge of whether or not an AWS is about to commit a crime. This is true because the future behaviour of a system will depend on both the influence of the commander and of the programmer. In the case of AWS, this further limits the remaining scope of command responsibility.

The programmer could, however, be culpable on the basis of superior responsibility. This is because the AWS's behaviour can only be limited through the combined influence of the commander and the programmer. The Rome Statute provides for criminal liability of civilian superiors, reliant on 'effective authority and control, and as a result of his or her failure to exercise control properly over such subordinates.'[918] Although there are similar challenges that could prevent the programmer from holding superior responsibility, such responsibility could potentially be expanded to offset the limitation of command responsibility, specifically because the parameter-setting piece, previously unique to the commander, will be shared with the programmer.

Barriers to the attribution of responsibility caused by AWS's discretional autonomy in terms of control and predictability are accurate objections to the way in which these technologies are developed and engaged. What is important here, is that the liability gap is noted along with the commander's loss of control over the system's behaviour.[919] Discretional autonomy could prevent AWS from acting as intended by their programmers or as ordered by their commanders. Programmers or commanders could even become unable to reliably forecast the system's actions or predict their consequences, constituting a failure to take necessary precautions and giving rise to arguments that these systems are ex ante unlawful.

However, such responsibility issues are circumstantial and centre on the systems' practical technological abilities and the way in which they are used. Therefore, according to this argument, the specific scenario in which an AWS is used will influence the distribution of responsibility for

[918] Rome Statute, Article 28(2).
[919] Herbert Hart, *Punishment and Responsibility: Essays in the Philosophy of Law* (Oxford University Press, 2008) 227.

the machine's actions, according to the specific requirements for control and prediction. However, if technology advances in such a manner that an AWS's actions become predictable, objections to assigning responsibility for these consequences to either the programmer or the commander will lose ground. The responsibility gap associated with the use of AWS would thus be narrowed. However, these shifting circumstances would barely affect the responsibility gap between the very notions of responsibility.

AWS and the Irrelevance of Command Responsibility

Although some commentators suggest that responsibility for an AWS's actions can be determined through the rules of command responsibility, [920] this work refutes this opinion. Those who deploy AWS are not necessarily commanders and AWS are neither agents nor combatants. Although it may not be intentional, academics who refer to commanders when discussing those who deploy AWS suggest that an AWS itself is a fighter or combatant. It is important not to consider these systems in this way. AWS are weapons and their development should not incorporate any functionality or autonomy that turns then into robotic combatants.

This work thus proposes that the notion of command responsibility is not relevant to, and should not be assigned to, AWS. ICL and IHL define command responsibility as a method of calculating criminal liability. This concept governs the relationship between human commanders and their human subordinates and had been introduced and developed as such. When describing an individual who deploys an AWS as a commander, academics mislead their audiences. The literal definition of a commander states that this individual exercises authority over their troops during military activities.[921] According to IHL and ICL, a commander is a human being who exercises authority over other human beings during military activities.[922] Similarly, Article 28 of the Rome Statute explains the notion of a commander by using terms such as 'forces' and 'subordinates', susceptible to both prosecution and punishment.[923] This notion alone demonstrates that the

[920] Nathan Reitinger, 'Algorithmic Choice and Superior Responsibility: Closing the Gap Between Liability and Lethal Autonomy by Defining the Line Between Actors and Tools' (2015) 51 *Gonzaga Law Review* 118; Jack Beard, 'Autonomous Weapons and Human Responsibilities' (2014) 45 *Georgetown Journal of International Law* 660.
[921] See <https://dictionary.cambridge.org/dictionary/english/commander> (accessed 21 May 2019).
[922] Michael Schmitt, 'Yamasihita, Medina, and Beyond: Command Responsibility in Contemporary Military Operations' (2000) 164 *Military Law Review* 176.
[923] See Article 28 of the Rome Statute.

individuals who drafted the Rome Statute intended for the concept of a commander to be premised by a human interaction.

Furthermore, by considering the elements of command responsibility, one can see that the concept was specifically developed to preside over the interaction between humans in combat. For a commander to be held accountable for their own actions or for those of their subordinates, three fundamental criteria must be met:

'i) That the commander knew or ought to have known that crimes were about to or were being committed by his or her subordinates;

ii) That the responsible commander failed to prevent or stop commission of the crimes by his or her subordinates;

iii) And that the commander did not punish the subordinate after the fact. '[924]

These criteria have been created and developed in international courts throughout the decades and are used as a framework of reference when seeking to establish command responsibility in court.[925] The first two criteria consider commanders and subordinates, concepts which have been consistently used to refer to human beings. Moreover, the third speaks of a commander's responsibility for the punishment of their subordinates, should they commit a crime. As previously discussed, machines have no moral compass. Further, they cannot suffer any form of punishment.[926] This clearly demonstrates that the introduction of command responsibility as a concept was intended to consider human interaction during conflict. Naturally, legal concepts are

[924] Article 28 of the Rome Statute; See also Article 86 (2) and 87 of Additional Protocol I to the Geneva Conventions.
[925] *Prosecutor v. Zdravko Mucic aka "Pavo", Hazim Delic, Esad Landzo aka "Zenga", Zejnil Delalic (Trial Judgement),* (International Criminal Tribunal for the former Yugoslavia, Trial Chamber, Case No IT-96-21-T, 16 November 1998); *Prosecutor v. Stanilav Galic (Trial Judgement and Opinion)* (International Criminal Tribunal for the former Yugoslavia, Trial Chamber, Case No IT-98-29-T, 5 December 2003) [173].
[926] Vivek Sehrawat, 'Autonomous Weapon System: Law of Armed Conflict (LOAC) and other Legal Challenges' (2017) 33 *Computer Law & Security Review* 23; Benjamin Kastan, 'Autonomous Weapons Systems: A Coming Legal Singularity' (2013) 45 *Journal of Law, Technology & Policy* 65; Chantal Grut, 'The Challenge of Autonomous Lethal Robotics to International Humanitarian Law' (2013) 18 *Journal of Conflict and Security Law* 15.

sometimes developed to encompass new circumstances. In the case of AWS and command responsibility, however, this is not an appropriate course of action.

Further, in terms of AWS and related command responsibility, Asaro notes 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.'[927]

The single scenario in which command responsibility would be relevant is if the commander or civilian supervisor responsible for the system's programming or deployment were aware, or should have been aware, that their subordinate was coding the system to behave in an illegal fashion and failed to prevent this or to punish their criminal behaviour.[928] The same reasoning applies equally to any other weaponry.

In this respect, this work proposes that AWS should be considered as weapons and their deploying humans as combatants. In a legal context, AWS are unable to, and should not, commit crimes. In the words of Seneca, 'a sword is never a killer, it is a tool in the killer's hands.'[929] As such, if this is true of combatants and their weapons, to determine a combatant's culpability for use of an autonomous system, criminal responsibility would provide the appropriate framework for doing so.[930] The above situation illustrates the full scope of command responsibility in relation to AWS. It is limited to situations in which a commander fails to deter, stop or punish the illegal use of AWS by their subordinates.

---

[927] Peter Asaro, 'On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-Making' (2012) 94 *International Review of the Red Cross* 701.
[928] See Michael Schmitt, 'Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics' (2013) *Harvard National Security Journal* 33.
[929] Quoted by Michael Schmitt, 'Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics' (2013) *Harvard National Security Journal* 1.
[930] Marco Sassòli, 'Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified' (2014) 90 *International Law Studies / US Naval War College* 324.

Nonetheless, as previously discussed, AWS offer significant barriers to the notion of individual criminal liability when they become either fully autonomous or autonomous to such an extent that their operator is no longer able to maintain 'meaningful human control'. In the case of AWS, meaningful human control by their operator is particularly relevant. However, according to Schmitt, it is possible to approach weaponry from a different angle:

'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. A human must decide how to program the system. Self-evidently, that individual would be accountable for programming it to engage in actions that amounted to war crimes.'[931]

Schmitt, like Sassòli, disregards any notion of unpredictability within fully or highly autonomous AWS operating in dynamic environments. If adhered to, his argument suggests that once an AWS has been programmed and deployed, the full range of its potential actions are then attributable to its deploying officer and its software programmer. As such, his argument proposes that an AWS's programming constitutes meaningful control over the weapon, creating responsibility for all subsequent acts. This proposal discards the crucial component of *mens rea* and replaces it with a form of 'strict criminal liability'. It proposes that every action of a pre-coded AWS can be forecast. Arguably, this is untrue. There are scenarios in which combatants who do not intend to act illegally could deploy an AWS to strike upon legitimate targets, only to find that the system then kills innocent civilians during the strike. Fully autonomous weapon systems, for instance, will make their own decisions after launch. These decisions may not comply with the intentions of their launching operator. This reality is intensified if the system has no requirement or capacity for human intervention after activation. In such scenarios, determining *mens rea* is particularly challenging.

Therefore, opposing Schmitt's apparent claims, the notion of control over a weapon appears central to an operator's responsibility for its actions. For such control to be meaningful, pre-programming alone is insufficient. The weapon also needs to be appropriately supervised, in real-time, once

[931] Michael Schmitt, 'Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics' (2013) *Harvard National Security Journal* 33.

activated. The behaviour of an AWS must be subject to strict human control, with the human operator approving target selections, preventing strikes and aborting missions as appropriate.
Consider for a moment the notion that one day, AWS will possess the sentient qualities of discretion and judgement, otherwise known as good faith and common sense. They would be used in conflict in place of human soldiers. They would be armed, make decisions on when to use force, and apply the LOAC principles of proportionality and distinction. No longer would they be weapons, operated by combatants. Instead, they would be combatants that operated their own weapons.

At this stage, AWS should be not be subject to weapon analysis or use of force analysis. Instead, they should be scrutinised as combatants. Assessed as such, AWS do not meet the legal criteria for a combatant and are not permitted to apply lethal force. LOAC empowers combatants to use lethal force.[932] Non-combatants do not have these permissions and their use of lethal force is considered an illegal act.[933] Article 43 of Additional Protocol I proposes a definition for armed forces, under which their members are considered combatants. It states:

'The armed forces of a Party to a conflict consist of all organized armed forces, groups and units which are under a command responsible to that Party for the conduct of its subordinates, even if that Party is represented by a government or an authority not recognized by an adverse Party. Such armed forces shall be subject to an internal disciplinary system which, inter alia, shall enforce compliance with the rules of international law applicable in armed conflict.'[934]

This provision contains two requirements that are challenging for AWS. The first is that the systems must operate under a command responsible to the party. Secondly, they must adhere to a disciplinary system and, as such, be subject to punishment.

[932] Geneva Convention Relative to the Treatment of Prisoners of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 135 (Third Geneva Convention).
[933] Nils Melzer, '*Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law'* (ICRC, 2009) available online <https://www.icrc.org/eng/assets/files/other/irrc-872reports-documents.pdf> accessed on 5 August 2018 at 24.
[934] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Additional Protocol I) art 43. See also Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law Volume I: Rules* (Cambridge University Press, 2009) 4.

In terms of the first requirement, it could be presumed that such systems would be used by a military force in the same way as human soldiers. As such, they would be expected to function in the same way under appropriate commanders. A commander, however, can discipline their troops, but would not be able to cause an AWS to change its behaviour if such conduct resulted from its software programming. In fact, these systems would obey their internal algorithms over the orders of their commanding human. Furthermore, a commander would probably hold no responsibility for an AWS's criminal actions. If an autonomous machine violated LOAC through a strike, by using disproportionate force, for example, matters of responsibility would become obscured. If such a violation resulted from a failure in its software, a human engineer or programmer involved in its design and development could be liable, as well as the those who performed its negligent test and evaluation during acquisition. Engineers and programmers are employed by system manufacturers and determine systems' behavioural models. These individuals are non-military personnel and do not form part of a command responsible to the party. Identifying those responsible for an AWS's actions will be, at best, a challenge. As such, autonomous weapon systems are not considered part of an armed force. Therefore, they are to be considered non-combatants which have not been granted the independent right to use lethal force.

In terms of the second requirement, it is important to consider whether or not a machine can adhere to a disciplinary system. If not, such systems cannot be considered part of an armed force and, as such, do not have the legal power to use lethal force. In order to satisfy this requirement, it must be possible to control the combatant, and the system must provide adequate means for achieving this. Disciplinary systems centre on the use of punitive measures to ensure adherence to rules and regulations. Software that determines robotic actions does not respond to disciplinary measures. No software that causes illegal conduct will be corrected until its coding is modified, its algorithms amended, or the values which are submitted to the algorithm changed. Only then would a different outcome be achieved. If any autonomous system were to violate its overarching rules and regulations, or commit crimes on account of poor programming, its logic or data will have failed. Software can be re-coded to address these shortcomings, but no commander can alter these logical deficiencies as and when they arise in the battlespace. The longer an AWS operates autonomously in-theatre, the greater the issue of its absent disciplinary system. This requirement specifies that

an operational commander can address and control any deviant behaviour. Any AWS with defective coding, however, would prevent a commander from exercising this disciplinary control. The more we seek to replace military personnel with AWS, the more complex this issue will become. Commanders may be left in a position where they have no option but to deploy an AWS. According to Article 43, the parties in any armed conflict must hold their personnel within a responsible command structure and disciplinary system that both seek to ensure LOAC compliance. As AWS to not fall under such structures, and are controlled by pre-coded software, they do not respond to punitive measures but, instead, to software re-engineering. Therefore, AWS should be considered non-combatants, lacking the right to exercise lethal force.

Manufacturer Responsibilities for AWS

Manufacturers and International Law

While it used to be said that international law applied only to states, and that corporations and other bodies sat outside of its remit,[935] there is now a general consensus that corporate liability has strong roots in international law.[936] Customary international law, the general principles of international law and numerous treaties all dispel the notion that commercial organisations have immunity under international law.[937] International law does not address corporations directly but international law requires states to take a range of actions with regard to such actors. In fact, States are not required by international law to grant commercial organisations the benefit of sovereign immunity under domestic law.For instance, Article 10 of the European Convention on the Prevention of Terrorism states that:

'1. Each Party shall adopt such measures as may be necessary, in accordance with its legal principles, to establish the liability of legal entities for participation in the offences set forth in Articles 5 to 7 and 9 of this Convention.

[935] Vikramaditya Khanna, 'Corporate Criminal Liability, What Purpose Does It Serve?' (1996) 109 *Harvard Law Review* 1489.
[936] Penelope Simons & Audrey Macklin, *The Governance Gap: Extractive Industries, Human Rights, and the Home State Advantage* (Routledge, 2014) 205; Juan Bohoslavsky & Jernej Cernic, *Making Sovereign Financing and Human Rights Work* (Hart Publishing, 2014) 63.
[937] Ralph Steinhardt, 'Weapons and the Human Rights Responsibilities of Multinational Corporations' in Stuart Casey-Maslen (eds), *Weapons under International Human Rights Law* (Cambridge University Press, 2014) 526.

2. Subject to the legal principles of the Party, the liability of legal entities may be criminal, civil or administrative.

3. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offences.'[938]

Quite specifically, treaties referencing the development, transfer and storage of specific weapon types do cover private industry. As such, they refer equally to corporations.[939] For instance, Article 9 of the 1977 Convention on the Prohibition of the Use, Stockpiling and Transfer of Anti-personnel Mines states that:

'Each state party shall take all appropriate legal, administrative and other measures, including the imposition of penal sanctions, to prevent and suppress any activity prohibited to a state party under this convention undertaken by persons or on territory under its jurisdiction or control.'[940]

Obviously, this is not an obligation imposed by international law on corporate entities. It is an obligation imposed on states to control the activities of a range of possible actors. Although corporate responsibility is detailed in international law, the non-human nature of a corporation raises a number of technical issues. In particular, when corporations are involved in weapon system production, the following questions arise:

---

[938] *Council of Europe Convention on the Prevention of Terrorism* art. 10, opened for signature May 16, 2005, C.E.T.S. No. 196; see also *United Nations Convention Against Transnational Organized Crime* art. 10, opened for signature Nov. 15, 2000, T.I.A.S. No. 13127, 2225 U.N.T.S. 209; *Convention on Combating Bribery of Foreign Public Officials in International Business Transactions* art. 2, opened for signature Dec. 17 1997, 2802 U.N.T.S.1; *International Convention on the Suppression and Punishment of the Crime of Apartheid* art. 1(2), Nov. 30, 1973, 1015 U.N.T.S. 243.

[939] *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction*, opened for signature Apr. 29, 1997, 1974 U.N.T.S. 469; Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and toxin Weapons and on Their Destruction, opened for signature Apr. 10, 1972, T.I.A.S. No. 8062, 26 U.N.T.S. 583.

[940] *Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-personnel Mines and Their Destruction* art. 9, opened for signature Sept. 18, 1997, 2056 U.N.T.S. 211.

In what circumstances is a parent company liable for acts performed by its partners, subsidiaries, distributors, contractors, or suppliers? In what circumstances is a company responsible for the behaviour of its human agents? For violations that require *mens rea*, how can a corporation be considered to have a mental state, and how can a prosecutor illustrate or prove this mental state? Even if a corporation were technically responsible for a legal violation, how could it be penalised without its innocent investors, employees, customers and public also being affected?

While many of these questions will long remain unanswered, the following discussion will seek to design a way out, paying particular attention to the responsibilities of those corporations that contribute to AWS design and production.

Criminal Responsibility of Manufacturer

Should an organisation develop or produce an AWS in such a way that it will violate international law, that organisation will be criminally liable for those violations.[941] There are a number of jurisdictions that support criminal sanctions for organisations that engage in criminal conduct.[942] For instance, a corporation could be charged with manslaughter. Punishments for manslaughter could include company deregistration, termination of an operating licence, or financial reparations.[943]

However, there is no universal consensus on corporate responsibility because some powers disprove of the notion that an entity 'with no soul to damn and no body to kick' might be effectively punished for any violations.[944] Moreover, in some jurisdictions, corporate responsibility is subject to a number of limitations. For instance, corporations can only be considered liable if the alleged legal actions were intended by top and senior executives, and not just a low-level employee or employees.[945]

---

[941] Erik Luna, 'The Curious Case of Corporate Criminality' (2009) 46 *American Criminal Law Review* 1507.
[942] Mark Pieth & Radha Ivory, *Corporate Criminal Liability: Emergence, Convergence and Risk* (Springer, 2011) 14. Example of such states are the US, Israel, France and the UK.
[943] Hilary Stauffer, 'Corporate Liability: An Alternative Path to Accountability?' in Stuart Maslen, Nathalie Weizmann, Maziar Homayounnejad, & Hilary Stauffer (eds), *Drones and Other Unmanned Weapons Systems under International Law* (Brill, 2018) 203; *The 2007 UK Corporate Manslaughter and Corporate Homicide Act*.
[944] Ralph Steinhardt, 'Weapons and the Human Rights Responsibilities of Multinational Corporations' in Stuart Casey-Maslen (eds), *Weapons under International Human Rights Law* (Cambridge University Press, 2014) 508.
[945] Nadia Bernaz, 'Corporate Criminal Liability under International Law: The New TV S.A.L. and Akhbar Beirut S.A.L. Cases at the Special Tribunal for Lebanon' (2015) 13 *Journal of International Criminal Justice* 315.

Additionally, if the alleged actions relate to government-sanctioned military activity or developments in public functions, corporate liability does not apply.[946] In jurisdictions such as these, the matter of corporate liability for AWS manufacturers will encounter the same restrictions.

Civil Responsibility of Manufacturer

When a crime has been committed, one potential remedy is for an offender to pay reparations to their victim. In this case, victims could sue those responsible for an AWS, including the individuals who contributed to its development, coding and manufacture and the state agents responsible for its deployment.[947] It could be difficult to hold a manufacturer to account, though, as such individuals may have no direct link with any of the victim's suffering. Liability is not normally attached to weapon manufacturers when those weapons are then used to commit offences. Moreover, 'product liability laws are largely untested in robotics.'[948] However, in some jurisdictions, there is a strict liability to supplying defective and dangerous products. For instance, in the US States, the immunity available to the manufacturer of weapons for the unlawful use of the weapon does not apply when the weapon itself is defective.[949] This will greatly complicate the task of any AWS victim who seeks to bring a civil lawsuit against a system manufacturer, unless that manufacturer has clearly acted with *mala fide* intent.

In the case of both corporate criminal responsibility and civil lawsuits, the onus is on victims to start claims. Typically, these claims are commenced in foreign jurisdictions.[950] As well as matters of financing, victims must overcome a range of jurisdictional complications and technicalities. Indeed, Heyns considered whether this approach might be unfair on victims.[951]

---

[946] For instance, *the 2007 UK Corporate Manslaughter and Corporate Homicide Act*.
[947] Steven Ratner et al, *Accountability for Human Rights Atrocities in International Law: Beyond the Nuremburg Legacy* (Oxford University Press, 2009) 355.
[948] Patrick Lin, 'Introduction to Robot Ethics' in Patrick Lin and others (eds), *Robot Ethics: The Ethical and Social Implications of Robotics* (MIT Press, 2012) 8.
[949] Benjamin Caryan, 'Held Accountable: Should Gun Manufacturers Be Held Liable for the Criminal Use of Their Products' (2020), 13 *Journal of Business Entrepreneurship & Law* 23 *Available at:* https://digitalcommons.pepperdine.edu/jbel/vol13/iss2/2.
[950] Richard Meeran, 'Tort Litigation Against Multinational Corporations for Violations of Human Rights' (2011) 3 *City University of Hong Kong Law Review* 5.
[951] A/HRC/23/47, Report of the UN Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions. Christof Heyns, para 79.

International law provides four specific entry points for corporate responsibility; these are design, manufacture, sale and supply, and use. These points will now be examined in turn.

Manufacturer Responsibility for AWS Design

In cases where AWS were specifically designed to violate IHL or IHRL or any other relevant laws, corporate responsibility for such violations would be clearly evident. For instance, this would apply to a corporation if it knowingly designed an AWS that would shut its human operator out while being unable to distinguish between combatants and non-combatants, or would perform illegal acts that cause unnecessary harm. At this stage, domestic law would typically provide the basis for corporate responsibility. Steinhardt notes, however, that AWS may not be specifically designed to perform IHL or IHRL violations; indeed, these weapons may possess:

'Sufficient dual uses to make them lawful at the design stage; moreover, the design of such weapons without the actual deployment or operational use of the weapon might belong in the realm of sadistic fantasy before it triggered legal sanction. The mens rea or mental state for a violation is generally a necessary but insufficient condition for liability in the absence of some actus reus.'[952]

As Steinhardt notes, there is a prominent argument about the dual use of an AWS.[953] Numerous AWS components perform dual purposes. As such, it is difficult, if at all possible, to force states to forbid the design of these components.[954] While his initial statement is supported, Steinhardt's claims about *mens rea* and *actus reus* are a little less clear. If there is a domestic sanction against AWS designs that violate international law, *mens rea* would be represented by the guilty mind that creates a non-compliant design. The *actus reus,* however, would be the act of physically designing that AWS. In this scenario, *actus reus* is, indeed, existent. With this in mind, designers could

[952] Ralph Steinhardt, 'Weapons and the Human Rights Responsibilities of Multinational Corporations' in Stuart Casey-Maslen (eds), *Weapons under International Human Rights Law* (Cambridge University Press, 2014) 531.
[953] Matthias Bieri & Marcel Dickow, Lethal 'Autonomous Weapon Systems: Future Challenges' (2014) Center for Security Studies, Analysis in Security Policy 3 available at <http://www.css.ethz.ch/publications/pdfs/CSSAnalyse164-EN.pdf> (accessed 21 May 2019).
[954] See presentation of Michael Biontino on behalf of the Foreign Office of Republic of Germany to the CCW Expert Meeting Lethal Autonomous Weapon Systems at page 3. Available at <http://www.unog.ch/80256EDD006B8954/%28httpAssets%29/6035B96DE2BE0C59C1257CDA00553F03/$file/Germany_LAWS_Technical_Summary_2014.pdf> (accessed 21 May 2019).

potentially be prosecuted before their non-compliant design was used to create an AWS, or the resulting AWS went on to commit a violation.

The Paradox of a Responsible Arms Maker

If a manufacturer elects to create illegal weapons, that manufacturer has a clear responsibility for this illegality.[955] This unlawfulness could be proven on the basis of treaty law that bans the creation or storage of the weapon in question.[956] Potentially, such a weapon could also violate customary international law.[957] Currently, there are no treaties that proscribe AWS and no consensus on the relevant provisions of customary international law. Should an AWS manufacturer provide a system which is not technically illegal, and this weapon is subsequently used in an illegal manner, the manufacturer will not 'trigger liability unless the company has substantial knowledge of the illegal use of that particular customer.' This is consistent with the previous discussion on different forms of perpetration, such as aiding and abetting and planning.[958] Hence, an Indian machete manufacturer, for instance, would not normally be held to account for the use of its machetes in Africa. However, if the manufacturer knew that these machetes would be used to decapitate civilians, it would be liable for aiding and abetting.[959]

Manufacturer Responsibility for AWS Sale and Supply

Treaty obligations, of course, stipulate that states are responsible for preventing the sale and supply of certain weapons.[960] As such, states are obliged to enforce suitable measures to control the actions of natural and legal persons, preventing them from violating the state's international obligations.[961] Therefore, if a corporation supports activity that does not comply with the state's international obligations, violating arms embargoes, for example, that state can then choose to sanction the corporation. Possible sanctions would include those previously discussed.

---

[955] *Treaty on the Prohibition of Nuclear Weapons*, July 7, 2017, 729 UNTS 161.
[956] E.g., *Convention on the Prohibition of the Use, Stockpiling, Production, and Transfer of Anti-personnel Mines and on their Destruction*, Sept. 18, 1997, 2056 U.N.T.S. 211.
[957] E.g., International Committee of the Red Cross [ICRC], Customary IHL Rule 74. Chemical Weapons, <https://ihl-databases.icrc.org/customary-ihl/eng/docs/vlrul-rule74> (accessed 8 May 2019).
[958] Ralph Steinhardt, 'Weapons and the Human Rights Responsibilities of Multinational Corporations' in Stuart Casey-Maslen (eds), *Weapons under International Human Rights Law* (Cambridge University Press, 2014) 531.
[959] Daniel Fischel and Alan Sykes, 'Corporate Crime' (1996) 25 *Journal of Legal Studies* 319.
[960] Edward Diskant, 'Comparative Corporate Criminal Liability' (2008) 118 *Yale Law Journal* 140.
[961] United Nations Legislative Series, Materials on the Responsibility of States for Internationally Wrongful Acts, at 51, U.N. Doc ST/LEG/SER.B/25 (2012).

Manufacturer Responsibility for AWS Use

If a corporation has direct involvement in armed conflict or the use of force, its liability will be explained in relevant guidelines. For instance, in terms of direct involvement in military operations, corporations are clearly liable for any weapons they use in combat.[962] If this weapon is used by other parties and not directly used by the corporation, this presents a different challenge. It is important, therefore, to consider whether a corporation could be liable for the military use of a weapon under the relevant *lex specialis*—international weapons law.

While corporate criminal liability is an important matter, it should not be combined with the individual criminal liability of the weapon operator or the law enforcement personnel previously mentioned.[963] AWS manufacturers and combatants should not divide or share their responsibility for its eventual use. To do so would be to dilute the legal responsibilities of a weapon operator.[964] Currently, no weapon operator would ever say, after committing a war crime, 'it was not me, something went wrong with my weapon; ask the manufacturer.' Weapon system manufacturers have specific responsibilities for the weapon's production. Similarly, combatants have their own personal responsibilities when operating their weapon systems. Nevertheless, corporation employees may hold individual criminal liability.[965]

Many academics have considered the notion that, under IHL, roboticists and others might be liable for AWS-related war crimes, even when their duties were performed before the outbreak of the relevant conflict.[966] Sassòli proposes that this issue is complex. He does, however, suggest that any individual who deliberately programs an AWS to commit violations will represent an 'indirect perpetrator of the war crime committed during the conflict.'[967] Should the AWS operator be

---

[962] *The Montreux Document on Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies During Armed Conflict*, ICRC and Swiss Federal Department of Foreign Affairs, Geneva (2009).

[963] See ICRC, Customary IHL Rule 151. Individual Responsibility, <https://ihldatabases.icrc.org/customary-ihl/eng/docs/v1_cha chapter43 rulel51> (accessed 8 May 2019).

[964] Michael Schmitt & Jeffrey Thurnher, 'Out of the Loop: Autonomous Weapon Systems and the Law of Armed Conflict' (2013) 4 *Harvard National Security Journal* 279.

[965] See ICRC, Customary IHL Rule 151. Individual Responsibility, <https://ihldatabases.icrc.org/customary-ihl/eng/docs/v1_cha chapter43 rulel51> (accessed 8 May 2019).

[966] Marco Sassòli, 'Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified' (2014) 90 *International Law Studies/Naval War College* 325.

[967] Marco Sassòli, 'Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified' (2014) 90 *International Law Studies/Naval War College* 325.

cognisant of the defect, the programmer in question will then represent an accessory to the crime.[968]

Although Sassòli's claims are correct, careful examination of the modes of responsibility presented at international courts and tribunals may suggest that the matter is not as complex as it first appears.[969] In order for an AWS manufacturer or roboticist to be indicted as an aider, abettor, or direct perpetrator of a war crime, they must be directly linked to the conflict and the prosecutor must prove *mens rea* and *actus reus*.[970] Without evidence of a direct link, the manufacturer or roboticist would need to be prosecuted under domestic criminal law.

To illustrate the above suggestion, consider a manufacturer who knows of an armed conflict that is either underway or impending. This manufacturer then creates and supplies AWS to one of the conflicting parties, in the full knowledge that this AWS will be used to commit war crimes.[971] In this scenario, the manufacturer is entirely comparable to political leaders like Charles Taylor who support the commission of crimes against humanity and war crimes.[972]

Such circumstances can also be seen in the British *Bruno Tesch et al* case where a company owner, Bruno Tesch, was charged with war crimes alongside his assistant Weinbacher, and gassing engineer Drohisn. In this case, the three supplied lethal gas to concentration camps[973] and the

[968] Marco Sassòli, 'Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified' (2014) 90 *International Law Studies/Naval War College* 325.
[969] Andre Klip & Steven Freeland, *Annotated Leading Cases of International Criminal Tribunals: The International Criminal Tribunal for the Former Yugoslavia* (Intersentia, 2001) 321. Klip and Sluite emphasise that 'the crux of attribution of responsibility over war crimes and other international crime is proving mens rea.'
[970] Tetyana Krupiy, 'Unravelling Organisational Power Dynamics: Towards a Theory of Accountability for Crimes Triggered by Lethal Autonomous Weapon Systems' (2017) 15 *Loyola University Chicago International Law Review* 19; *Bruno Tesch and Others (Zyklon B Case)*, UNWCC, Case Number 9, British Military Court (1946), Law Reports of Trials of War Criminals (1949) Volume 1, 93104.
[971] See cases of *The United States of America v Carl Krauch, et al*, 1168 -72; *Bruno Tesch and Others (Zyklon B Case)*, UNWCC, Case Number 9, British Military Court (1946), Law Reports of Trials of War Criminals (1949) Volume 1, 93-104.
[972] *Prosecutor v Taylor (Judgement)* (Special Court for Sierra Leone, Trial Chamber II, Case No SCSL-03-01-T, 18 May 2012).
[973] See case of *Bruno Tesch and Others (Zyklon B Case)*, UNWCC, Case Number 9, British Military Court (1946), Law Reports of Trials of War Criminals (1949) Volume 1, 93-104; Mohamed Badar, *The Concept of Mens Rea in International Criminal Law: the Case for a Unified Approach* (Hart Publishing, 2013) 234.

charge stated that they knew how the gas would be used.[974] Because the three individuals knowingly provided gas to a state organisation that used it to commit war crimes, the prosecution argued that they were, indeed, war criminals.[975] Although the gas formulas or gas itself may have been created before the start of the war, the accused still had a direct link to the war crime and *mens rea*, meaning that the timeline would not excuse them of their responsibilities.

In another such scenario, a manufacturer might create and sell AWS to a customer who is already involved in an armed conflict or later becomes involved. The manufacturer does not, in this example, know that the AWS will be used to commit war crimes. Indeed, the manufacturer would not be liable for prosecution for the war crimes, as *mens rea* must be proven for the specific, alleged war crime.[976] Nevertheless, if that AWS were illegal in its design, the manufacturer may still be prosecuted under domestic criminal law.

This justification formed the basis of the defence argument for *Bruno Tesch et al*. In theory, they correctly affirmed that prosecution for war crimes must be specific. As such, specific intent is required. The prosecutors could not simply claim that the accused were guilty of supplying toxic gas; to consider them a party to the war crime they needed to, instead, prove that the individuals had the specific intention of supporting deaths in the concentration camps. Without such proof, 'to supply material which also had quite legitimate purpose is no war crime.'[977] The court agreed in principle with the defence counsel, stating that the accused would not be convicted of war crimes without three levels of proof. The first was proof that individuals in the camps were killed using toxic gas. The second was that the accused did supply this gas. The third was that, at the point of supply, the accused knew how the gas would be used.[978]

---

[974] See case of *Bruno Tesch and Others (Zyklon B Case)*, UNWCC, Case Number 9, British Military Court (1946), Law Reports of Trials of War Criminals (1949) Volume 1, 93-10; Iryna Marchuk, *The Fundamental Concept of Crime in International Criminal Law: A Comparative Law Analysis* (Springer, 2013) 134.

[975] See case of *Bruno Tesch and Others (Zyklon B Case)*, UNWCC, Case Number 9, British Military Court (1946), Law Reports of Trials of War Criminals (1949) Volume 1, 94.

[976] See *the United States of America v Carl Krauch, et al*, 1168 -72.

[977] See case of *Bruno Tesch and Others (Zyklon B Case)*, UNWCC, Case Number 9, British Military Court (1946), Law Reports of Trials of War Criminals (1949) Volume 1, 98; Jose Doria et al, *The Legal Regime of the International Criminal Court: Essays in Honour of Professor Igor Blishchenko [1930-2000]* (Brill, 2009) 144.

[978] See case of *Bruno Tesch and Others (Zyklon B Case)*, UNWCC, Case Number 9, British Military Court (1946), Law Reports of Trials of War Criminals (1949) Volume 1, 101; See Mohamed Badar, *The Concept of Mens Rea in International Criminal Law: the Case for a Unified Approach* (Hart Publishing, 2013) 234.

Similarly, in the *IG Farben* case at the Trials of War Criminals before the Nuremberg Military Tribunals, company employees were charged with crimes against humanity and conspiracy to commit war crimes. IG Farben was a multinational corporation of chemical companies. The corporation's Director of Agfa-Gevaert NV, Chief Counsel and Head of Legal, Head of Chemical Research, Head of Department responsible for nitrogen and gasoline production, Head of Pharmaceuticals, and intelligent plant police officers were all accused of supporting war crimes by providing the poison gas used in extermination camps, *Zyklon B*. After the tribunal determined that the individuals were unaware of the intended illegal use for the gas, the accused were all acquitted.[979]

These cases highlight an important fact: suppliers of lawful materials could be found guilty of war crimes, provided they are proven to have known that the material would be used for an unlawful purpose.[980]

Product Liability

To date, '[p]roduct liability laws are largely untested in robotics.'[981] This is certainly true of AWS. Undeniably, although some factions have referred to product liability as a practicable alternative to individual and State responsibility.[982] As the primary concepts of interest are largely overseen by domestic law (excluding European Directive 85/374/EEC),[983] it is not possible to present an in-depth clarification of the issue in the confines of this section. As such, we will reduce the scope to some more general observations.

Notwithstanding the unquestionable (and often philosophical) variations in the distinct legal systems that have been implemented throughout the world, product liability mechanisms typically

[979] See the case of *The United States of America v Carl Krauch, et al*, 1168 -72.
[980] See the case of *The United States of America v Carl Krauch, et al*, 1168 -72; *Bruno Tesch and Others (Zyklon B Case)*, UNWCC, Case Number 9, British Military Court (1946), Law Reports of Trials of War Criminals (1949) Volume 1, 93-104.
[981] Patrick Lin, 'Introduction to Robot Ethics' in Patrick Lin and others (eds), *Robot Ethics: The Ethical and Social Implications of Robotics* (MIT Press, 2012) 8.
[982] Armin Krishnan, *Killer Robots: Legality and Ethicality of Autonomous Weapons* (Ashgate, 2009) 103; NATO Joint Air Power Competence Centre (JAPCC). 2016. *Future Unmanned System Technologies. Legal and Ethical Implications of Increasing Automation*. Kalkar (Germany): JAPCC 29.
[983] *The 1977 European Convention on Products Liability in regard to Personal Injury and Death* was signed by only 4 States and ratified by none.

adopt a plaintiff-friendly form; i.e., they establish the fault element level at a predetermined test of negligence and, in certain situations, transfer the burden of proof from the party that sustained the damage, to the defending company, which relies on that company demonstrating the applicability of one of the justifications granted under the law.[984] If we take into consideration the complexities surrounding the consider the proof of the fault aspect in AWS-related incidents, it becomes apparent that this aspect of the product liability regimes could be a major source of advantage to the party that sustained the damage.

However, legislative and theoretical boundaries can prevent victims from achieving redress. While the evidentiary system could provide the plaintiff with an advantage, product liability remains correlated with the defendant's negligent actions. Regardless of how low this is, the standard dictates that the malfunction that is the subject of the complaint should, at a minimum, have been conceivable by the company or individuals responsible for the product.[985] However, as consistently outlined, this is precisely what autonomy in AWS is destined to rule out in the majority of the incidents that lead to destructive events. Furthermore, some scholars have directly questioned the option of treating robots, including AWS, as products from a legal perspective and, as such, treating any detrimental decisions as defects. This argument is put forward on the basis that, to the degree that a robot possesses learning competences and the ability to make autonomous decisions, 'it is hardly plausible that [it] was defect; it did what it was supposed to do: It reacted to new inputs and adapted its behaviour – thus the machine is not defective as such.'[986]

Furthermore, it is important to take into consideration the fact that the United States is likely to be the largest manufacturer and deployer of AWS. However, in the courts of this country, product liability lawsuits are not permitted under the 'government contractor' defence, which emerged following the ruling of the US Supreme Court in the *Boyle* case.[987] According to this line of

[984] American Law Institute 1998, *Restatement of the Law, Third, Torts: Products Liability*, para. 3 (Circumstantial Evidence Supporting Inference of Product Defect).
[985] American Law Institute 1998, *Restatement of the Law, Third, Torts: Products Liability*, para. 2(b) ('[A product] is defective in design when the foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design'); Directive 85/374/EEC, Article 7 ('The producer shall not be liable […] if he proves: […] e) that the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered').
[986] Susanne Beck, 'The Problem of Ascribing Legal Responsibility in the Case of Robotics' (2015) 31 *AI & Society* 475.
[987] 487 U.S. 500 (1988).

defence, military contractors are protected against product liability in situations in which the product in question, which includes weapons systems, has been produced per the specifications handed down by a federal or state government agency. Such a situation is highly likely with AWS on the basis of the complex and delicate nature of the activities they are designed to conduct. Additionally, the scope of this defence has been consequently extended by federal courts such that it is now applicable in fundamentally every case that examines the misconduct of AWS. For example, in *Koohi v. United States et al.*, which concerned a precursor of contemporary AWS in the form of the Aegis air defence system, the Court of Appeals ruled that this doctrine should be applied to protect contractors from claims for damages 'arising out of the combatant activities of the military or naval forces […] during time of war'[988]—essentially, how AWS are projected to act in the not-too-distant future.

No-Fault Liability

The challenges that are described above could potentially be overcome through the implementation of a no-fault liability system. The introduction of a regime of this nature could be suitable in situations in which an inquiry pertaining to the fault aspect is especially complicated. Besides, there is a broad tendency to implement regimes of this nature at both the national and international levels with regards to the implementation of actions that may ultimately be found to be particularly hazardous due to their intrinsic nature or because of the means by which they are typically implemented.

No-fault liability is frequently cited in the domain of environmental law,[989] as can be observed in Article III of the International Convention on Civil Liability for Oil Pollution Damage (CLC):

'The owner of a ship at the time of an incident […] shall be liable for any pollution damage caused by oil which has escaped or been discharged from the ship as a result of the incident.'

[988] 976 F.2d 1328 (1992), 1337.
[989] Alex Kiss and Dinah Shelton, 'Strict Liability in International Environmental Law' in Tafsir Malick Ndiaye and Rüdiger Wolfum (eds), *Law of the Sea, Environmental Law and Settlement of Disputes: Liber Amicorum Judge Thomas A. Mensah* (Brill, 2007) 1148.

The logic that underpins this type of tenet can be traced back to the need to alleviate the community of the cost burden of environmental harm by transmitting responsibility to the entity or individual who benefited from the action that caused the harm.[990]

The implementation of a liability regime of this nature would undoubtedly be prudent with regards to the damages that can be attributed to AWS. After all, the use of an AWS on the battlefield could be rightly classified as 'ultra-hazardous', as 'it involves a risk of serious harm that cannot be eliminated, even if utmost care is exercised.'[991] Therefore, from a *de lege ferenda* standpoint, one could envisage a treaty instituting, in line with the CLC, a rule that the organizations and individuals that are responsible for the development and manufacture of AWS are legally required to compensate for any damages they cause.

Summary

The standards related to the prohibition of international crimes are often targeted at corporations. However, there is an absence of international forums that have sufficient authority over corporate crimes.[992] That said, there is an inherent need to examine this concept from the perspective of national courts, as the matter is likely to be considered within the context of tort liability.

It could be possible to reduce the responsibility gap that stems from the 'many hands' problem in cases involving international crimes that are executed by AWS through the lens of corporate tort liability. As previously described, if the execution of an international crime can be traced back to the collective action of a group of people—for example, a team of software programmers—it would be very difficult to allocate responsibility for the crime on an individual level. However, if accountability could be allocated at the corporate level, the evidentiary and abstract barriers could

[990] Alex Kiss and Dinah Shelton, 'Strict Liability in International Environmental Law' in Tafsir Malick Ndiaye and Rüdiger Wolfum (eds), *Law of the Sea, Environmental Law and Settlement of Disputes: Liber Amicorum Judge Thomas A. Mensah* (Brill, 2007) 1148.
[991] Rebecca Crootof, 'War Torts: Accountability for Autonomous Weapons' (2016) 164 *University of Pennsylvania Law Review* 1395.
[992] 'Article 21 of the ICC Statute, which rules out the Court's jurisdiction over legal persons, including corporations. It has been carefully demonstrated, however, that this limitation was due to reasons other than the their (alleged) lack of legal personality under international criminal law.' Andrew Clapham, 'The Question of Jurisdiction Under International Criminal Law Over Legal Persons: Lessons from the Rome Conference on the International Criminal Court' in Menno Kamminga and Saman Zia-Zarifi (eds), *Liability of Multinational Corporations Under International Law* (Kluwer Law International, 2012) 195.

be eradicated by relying on the 'collective knowledge' principle, which 'merely requires that the members of the company had knowledge in the aggregate.'[993] Specifically, while corporate entities don't have a distinct conscience, the involvement of the corporation in the execution of brutal crimes is often indicative 'of a systemic issue that proliferates throughout the corporate culture of the organization.'[994]

While this represents a clear benefit, even this particular path to accountability is replete with difficulties. The Alien Tort Statute is a very specific piece of legislation that clearly asserts tort liability for international crimes. However, this is not without its critics and it can only enforceable by US courts; there is no guarantee that it will emerge in additional jurisdictions.[995] In addition, if any call for damages questions the legitimacy (or even the suitability) of the military decisions that are made by the forum State, there is a high risk that jurisdiction will be declined by the court on the foundation of jurisprudential policies that aim to isolate matters of defence and foreign affairs from judicial enquiry (political question, non-justiciability, *acte de gouvernement* doctrines). Finally, although corporate tort liability for international crimes (and the associated 'collective knowledge' concept), constitutes a feasible remedy to the many hands issue, it does not entail that a criminal *mens rea*, in the manifestation of *dolus directus* or *indirectus*, does not need to be proven. Correspondingly, the issues that can be traced back to the intrinsic unpredictability of AWS remain unsettled.

Conclusion

It has been argued that AWS are controlled by a number of parties, including but not limited to programmers, roboticists, and manufacturers.[996] As such, it is important that the attribution of

[993] Caroline Kaeb, 'The Shifting Sands of Corporate Liability Under International Criminal Law' (2016) 49 *The George Washington International Law Review* 396.
[994] Caroline Kaeb, 'The Shifting Sands of Corporate Liability Under International Criminal Law' (2016) 49 *The George Washington International Law Review* 385.
[995] Elizabeth Fuzaylova, 'War Torts, Autonomous Weapon Systems, and Liability: Why a Limited Strict Liability Tort Regime Should Be Implemented' (2019) 40 *Cardozo Law Review* 1356; Beth Stephens, 'Translating *Filártiga*: A Comparative and International Law Analysis of Domestic Remedies for International Human Rights Violations' (2002) 27 *Yale Journal of International Law* 57.
[996] A/HRC/23/47, Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Christof Heyns, 2013 para 79.

responsibility for AWS actions considers a number of individuals.[997] Consequently, some researchers have proposed that these individuals should split and share responsibility for AWS actions.[998]

In 2014, at the Convention on Certain Conventional Weapons expert meeting on AWS, it was proposed by the US delegation that 'meaningful human control' begins when AWS components are manufactured, their software is programmed, and the eventual system is deployed.[999] As such, it was suggested that in considering the 'meaningful human control' of AWS, the discussion should 'capture the full range of human activity that takes place in weapon 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.'[1000]

Although split responsibility may be an appealing solution, it represents a misdirection. As previously explained, these individual parties have their own, distinct responsibilities for an AWS, whether that be through corporate responsibility or operational command. Between these responsibilities, it is not possible to 'split responsibility', *per se.* There is another example regarding split responsibility. If a member of the armed forces deploys an AWS and it will target civilians because of a defect in its programming. In this case, a member of the armed forces has no criminal ability due to a lack of *mens rea*. There are three possible options. First, the state may be responsible if it knew or ought to have known of the flaw. Second, the manufacturer may be responsible. Third, the operator has no responsibility unless he knew or ought to have known of the risk. The operator is entitled to assume that a legal review conducted for all weapons to ensure that their intended use is consistent with the laws of war. Specifically, when considering the matter

[997] A/HRC/23/47, Report of the UN Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Christof Heyns, para 81.
[998] A/HRC/23/47, Report of the UN Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Christof Heyns, para 81; Robert Sparrow, 'Killer Robots' (2007) 24 *Journal of Applied Philosophy* 24.
[999] US Delegate closing statement at the CCW Informal Meeting of Experts on Lethal Autonomous Weapon Systems (2014) Audio available at <http://www.unog.ch/80256EDD006B8954/%28httpAssets%29/6D6B35C716AD388CC1257CEE004871E3/$file/1019.MP3> (accessed 1 May 2019).
[1000] US Delegate closing statement at the CCW Informal Meeting of Experts on Lethal Autonomous Weapon Systems (2014) Audio available at <http://www.unog.ch/80256EDD006B8954/%28httpAssets%29/6D6B35C716AD388CC1257CEE004871E3/$file/1019.MP3> (accessed 1 May 2019).

of a combatant's responsibility for their weapon, this responsibility cannot be split or shared between the combatant and the system manufacturer, for instance. When holding a combatant to account for war crimes, IHL and international criminal law do not consider the manufacturer of any related weapon.[1001] The reason for this distinction is that the combatant decides which weapon to use and has control of the weapon at the time. Naturally, as previously discussed, manufacturers could be considered aiders, abettors, or co-perpetrators if the correct conditions are met. These liabilities, however, do not split the responsibility; individuals are separately liable for their own roles in the crime.[1002] Similarly, the same justification applies to corporate responsibility.

The suggestion of a 'split responsibility' option for AWS use by combatants is dangerous. It attempts to combine different modes of responsibility including corporate, command, and individual responsibility. In terms of IHL, civilian organisations are not involved in armed conflict unless they are direct participants.[1003] This body of law concerns weapons and combatants, not weapon manufacturers or any other such party who may contribute to their production, save for situations where they then play a direct role in the conflict.[1004]

[1001] See Geneva Academy of International Humanitarian Law 'Autonomous Weapon Systems under International Law' (2014) 8 Academy Briefing Number 25 noting that 'for violating the fundamental principle that no penalty may be inflicted on a person for an act for which he or she is not responsible.' See 1907 Hague Regulations, Article 50; 1949 Geneva Convention IV, Article 33(1); 1977 Additional Protocol I, Article 75(4)(b); 1977 Additional Protocol II, Article 6(2)(b); ICRC Customary IHL Study, Rule 102.
[1002] See Article 25 of the Rome Statute.
[1003] Timothy McCormack & Avril McDonald, *Yearbook of International Humanitarian Law* (T.M.C. Asser Press, 2006) 84.
[1004] Timohy McCormack & Avril McDonald, *Yearbook of International Humanitarian Law* (T.M.C. Asser Press, 2006) 84.

Conclusions and Recommendations

This research has demonstrated that, on the whole, IHL offers no insuperable obstacles in terms of continuing the development and deployment of AWS. Extant regulations that apply to types and usage of weaponry are equally applicable to AWS as to other forms of weapon. States that continue to follow international regulations in the development, deployment and operation of more autonomous weaponry will not transgress IHL requirements. The primary legal difficulty is to forge an understanding of the ways in which current legal standards should be interpreted as weapons become increasingly autonomous.

In light of the substantial controversies that surround this issue, certain parties may regard such statements as endorsing further development of AWS, but this is not so. This dissertation offers neither endorsement nor opposition to developing or deploying AWS. The dissertation's intention has been to illustrate those legal considerations that come into play if further development of AWS occurs. This dissertation was never intended to offer an argument either positive or negative any one course of action in this area.

Decisions regarding the development and deployment of AWS must take into account many matters both within and outside IHL, such as morals and ethics as a source of law in the light of the Martens clause, strategy, security, politics, and the wider legal picture, especially in terms of human rights law. These issues are outwith the remit of this project.

On the basis of this specific research, two recommendations can be offered. Firstly, we may establish a definition of autonomy with regard to weapon systems that examines legality and

encourages constructive discussion. Secondly, we may offer an initial outline for a form of regulation that could encompass the chief areas of concern detailed above.

Both defensive weapons and offensive weapons have increasingly been employing autonomy over recent decades. Despite the pace of development, no internationally agreed standard for what defines an autonomous weapon currently exists. This is due to the fact that any useful definition must clearly distinguish between current weapons that have autonomous elements and the autonomous weapons we may see in future. In this dissertation, autonomous weaponry is defined as that which can select and engage a target or targets independently of additional human intervention. All governmental, expert and NGO definitions currently regard this as the essential feature of autonomous weaponry, that, weapons are only autonomous if humans have no input into the crucial choice of whether or not to use lethal/potentially lethal force. The choice in this context is that of making decisions regarding the selection and attack of target. This may refer to the weapon autonomously selecting and engaging targets, or the entire loop of targeting in which humans play a crucial part. From an international humanitarian law point of view, it is more useful for the latter interpretation to be used, so that it incorporates all the processes involved in the run-up to target selection and attack, such as selecting objectives, choosing targets, selecting weapons, and planning implementation; all these processes must have due regard for the possible damage to non-combatants.

It is highly likely that in the near future autonomous weaponry will be developed and employed for specific tasks, both defensive and offensive. Because autonomous systems can collect and process data much more swiftly than human operators and so are better able to defend against threats such as incoming missiles, and because they can partially eliminate the need for human soldiers on battlefields, particularly in areas that threaten human life, and so cut the danger to friendly soldiery and also because they have the potential to lower civilian casualty rates. If any state wishes its armed forces to keep up with technological development, autonomous weaponry must become a part of their armoury. However, deploying this type of weaponry must retain at least an element of substantive human control.

It may seem absurd to discuss substantive human control when we are referring to fully autonomous weaponry; surely if substantive human control is present, the weapon cannot be fully autonomous? In practice, substantive human control means that certain essential elements of weapon systems cannot become fully autonomous, with substantive human control being important in a number of phases of target selection. There are a number of points where humans will take decisions regarding the force to be employed and the extent to which it can be used, either in setting the rules of engagement, choosing to deploy autonomous weaponry, or programming the weaponry to select targets. This generally will mean that a number of people can be held to account in terms of their decision-making. The operator responsible for the activation of autonomous weaponry and the commander who ordered its deployment both have accountability in this area. In addition, a commander can be held responsible for any violations of humanitarian law committed by those under his/her command if inadequate levels of supervision can be demonstrated. However, the commander is not responsible for what that AWS does, he/she knew or ought to have known that it would do that. The fact that decisions have to be taken at a number of levels in order to implement targeting of autonomous weaponry may be regarded as reducing its associated risks, specifically those regarding its set areas of autonomy, the environment in which it operates, for how long it will be deployed and over what range it may operate.[1005] The greater the limitations imposed on the tasks of the weaponry, the lower the levels of dynamism it is permitted within its operational environment, the less time it is deployed, and the greater the limitations on mobility imposed, the easier it is to predict the effect of it being deployed. In these scenarios, the level of human control is higher. Contrastingly, more complex weaponry that swiftly moves across a range of fast-changing environments over a longer period will be more likely to act in unpredictable or unexpected ways. This lessens the levels of human control. However, even once the weaponry has undertaken an attack humans are still involved at the last stage of targeting, such as assessing the autonomous weaponry's performance, accuracy, and giving feedback on it; this will remain an important human control element.

[1005] Neil Davison, Characteristics of Autonomous Weapon Systems, Presentation made at the informal expert meeting organized by the state parties to the Convention on Certain Conventional Weapons 14 April 2015, Geneva, Switzerland, available at <www.unog.ch/80256EDD006B8954/(httpAssets)/37D5012BBF52C7BBC1257E2700599465/$file/Characteristics+of+AWS+ICRC+speaking+points+14+Apr+2015.pdf>.

While humans remain responsible for taking decisions related to autonomous weaponry deployment, no loopholes regarding autonomy in respect of AWS exist within IHL. At present, current legal standards have sufficient safeguards to enforce accountability in this area. It is unlikely that the criminal liability of a commander, military operative, politician, or programmer will be eroded over the next 10 years. They will retain responsibility for making decisions regarding the deployment and activation of autonomous weaponry in any particular scenario and for deciding if those decisions accord with IHL and have ethical justification. Similarly, there are no loopholes for the responsibility of a state that deploys autonomous weapons. Nevertheless, in comparison to deploying weaponry that must be continuously operated by a human being, such as a manned fighter aircraft or a tank, with autonomous weaponry the burden of accountability is somewhat shifted, because deploying autonomous weaponry does not require the selection of a particular target; target selection becomes an implicit part of the deployment and activation decision. This means that accountability rests essentially with the commander who made the choice of deployment and the operative responsible for activation, rather than a traditional soldier selecting and attacking a particular target. This will require commanders and operatives engaged in the deployment of autonomous weaponry to have high levels of training and information regarding possible outcomes of their decisions. Commanders and operatives will have to make reasoned choices as to precautions, proportionality, and distinction of targets with no specific knowledge of the target that will be chosen. This means substantive human control must be present in all phases of targeting. The essentials of IHL remain applicable to the regulation of autonomous weaponry deployment. If such deployment is noncompliant with these essentials, it is in breach of the law. Thus, a commander could have responsibility for recklessly deploying autonomous weaponry if such a deployment causes breaches of IHL. Commanders will have to be more restrained in the way they deploy such weapons, taking into account the complexities of such weaponry and the time gap between the weapon being activated (which is the last chance to take precautions and consider distinction and proportionality) and the attack being made. Nevertheless, commanders will not be able to abrogate their responsibility by claiming that any illegal outcomes resulting from their decisions could not be foreseen.

Internationally, there seems to be general agreement that the idea of meaningful human control is a useful one. While, at present, no definition of it is generally agreed, it is generally recognized

that it is a useful benchmark for creating distinctions between allowable and illegal forms of autonomous weaponry and the ways such weaponry should be deployed. It appears to be a broad enough definition that it can simultaneously address concepts of human dignity – which call for greater restriction – and the need to find a balance between total prohibition or total acceptance of such weaponry.[1006] It is apparent that such a compromise could be reached; for example, at the 2015 CCW conference regarding autonomous weaponry, Germany released a final statement stating that it 'will not accept the decision over life and death is taken solely by an autonomous system without any possibility for human intervention.'[1007] Commentators have noted that such a statement 'leaves significant space for requiring different levels of control and for demarcating critical functions that would require high levels of human control from less critical functions that would require lower or no direct human control.'[1008]

The primary difficulty now comprises how we determine the level and type of meaningful human control that should exist with autonomous weaponry and in identifying the crucial sections of the targeting process in which humans must retain substantial control. With regard to this, those participating in CCW meetings ought to come to agreement as quickly as possible that the underlying principle of any future regulation is that all decisions related to critical functioning and so essential legal issues, such as the right to life and bodily integrity, cannot be placed completely under the control of fully autonomous weaponry. Life and death decisions should come under substantive human control at all times, i.e., they must be ultimately taken by a human being. It would be useful if the members of the European Union could agree to a unified position regarding these issues.

In future CCW meetings and other fora, states ought to be advocating that at a national level procedures regarding Article 36 of the First Additional Protocol to the Geneva Conventions should

[1006] Nehal Bhuta, Susanne Beck and Robin Geiss, 'Present Futures: Concluding Reflections and Open Questions on Autonomous Weapons Systems' in Nehal Bhuta et al. (eds), *Autonomous Weapons Systems: Law, Ethics, Policy* (Cambridge University Press, 2016) 382.
[1007] Final Statement by Germany, CCW Expert Meeting on Lethal Autonomous Weapons Systems, 13–17 April 2015, Geneva, available at <www.unog.ch/80256EDD006B8954/(ht tpAssets)/07006B8A11B9E932C1257E2D002B6D00/$file/2015_LAWS_MX_Germany_ WA.pdf>.
[1008] Nehal Bhuta, Susanne Beck and Robin Geiss, 'Present Futures: Concluding Reflections and Open Questions on Autonomous Weapons Systems' in Nehal Bhuta et al. (eds), *Autonomous Weapons Systems: Law, Ethics, Policy* (Cambridge University Press, 2016) 382.

be more widely implemented, that the results of implementation should be shared in a more transparent manner, and that more information should be shared between states. Article 36 should be rigorously applied in any autonomous weaponry procurement process, and meaningful human control should be the gold standard of any such process.

In view of how important it is to attribute accountability and responsibility, states that procure autonomous weaponry must make sure that moral responsibility is incorporated into the engineering process during design and that extensive weapons testing takes place in the most realistic possible environments. States should also insist that when military personnel, particularly commanders, are trained in the ethics of warfare, issues concerning the deployment of autonomous weaponry are addressed.

Internationally (particularly in the context of the CCW), states should be promoting processes that will culminate in either a framework for an international convention to be formulated or, at least, a guide to interpretation being produced that offers clarification of the current legal position regarding deploying autonomous weaponry. Any document of this nature should, amongst other things, enumerate best practice regarding meaningful human control as set out in Article 36 as it relates to the deployment of autonomous weaponry.

Less specifically, states should continue to have active involvement in discussions within the CCW context regarding the implications of autonomous weaponry development legally, ethically, and in terms of policy. In relation to this, states should stress that the positive and negative aspects of such technologies must be publicly debated. This will allow states to remain in close contact with NGOs, scientists, and other concerned entities in this area.

AWS is obviously a divisive issue, and there is much uncertainty regarding its future due to the rapid nature of technological evolution. Nevertheless, if we accept that AWS is inevitable, that the weaponry has the potential for lawful use, and that when used properly they could reduce civilian casualties, then it is arguable that the optimal approach to the lack of agreement and standardization in this area is to publish a non-binding IHL Manual. Organizations such as NATO could build on the previous success of such Manuals, e.g. *Tallinn*, *San Remo* and *AMW*, by convening groups of

experts from the military, software engineers, weapons designers, roboticists, cognitive scientists and lawyers. Such groups would ideally have every state equally represented, although it is probable that a small group of developed states would contribute the majority of experts on international law, weapons design, and robotics. Furthermore, those states that are demanding a ban will probably not wish to provide any experts or even recognition for such a project, and NGOs would probably offer active opposition to it. This makes it even more essential for those convening such a group to persuade the ICRC to join, thereby providing the AWS Manual with greater legitimacy. Although the ICRC appears to be reticent, it may be willing to have a cautious involvement, potentially because it recognizes that AWS are inevitably going to become part of the battlefield and so it may wish to take advantage of the process to ensure there is a humanitarian input. There is a strong case to be made for welcoming such involvement, provided it does not disturb the sensitive equilibrium of military necessity and humanitarian considerations. Involving the ICRC could be a crucial step in gaining wider recognition for an endeavour that is likely to be strongly opposed by many NGOs.

Bibliography

Treaties and International Documents

Armed Forces Documents

‘Legal Review of New Weapons’ (Defence Instruction (General) OPS 44-1, Australian Department of Defence, 2 June 2005)

‘Network Enabled Capability’ (JSP 777 ed 1, United Kingdom Ministry of Defence, 2005) <http://webarchive.nationalarchives.gov.uk/20121026065214/http://www.mod.uk/NR/rdonlyres/E1403E7F-96FA-4550-AE14-4C7FF610FE3E/0/nec_jsp777.pdf>

‘Unmanned Systems Safety Guide for DoD Acquisition’ (United States Department of Defense, 27 June 2007) <https://acc.dau.mil/adl/enUS/683704/file/75176/Unmanned%20Systems%20Safety%20Guide%20forDOD%20A cquisition,27June%202007.pdf>

Belgium, Law of War Manual (1983) Droit Pénal et Disciplinaire Militaire et Droit de la Guerre, Deuxième Partie, Droit de la Guerre, Ecole Royale Militaire, par J. Maes, Chargé de cours, Avocat-général près la Cour Militaire, D/1983/1187/029, 1983.

Canada, Use of Force for CF Operations, Canadian Forces Joint Publication, Chief of the Defence Staff, B-GJ-005-501/FP-001, August 2008, § 105.6.

Cummings, Mary and Angelo Collins, ‘Autonomous Aerial Cargo/Utility System (AACUS)’ (Concept of Operations, Office of Naval Research)

<http://www.onr.navy.mil/~/media/Files/Funding-Announcements/BAA/2012/12-004CONOPS.ashx>

Defense Science Board, 'Patriot System Performance' (Report Summary, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, January 2005) <http://www.dtic.mil/get-tr-doc/pdf?AD=ADA435837>

Defense Science Board, 'The Role of Autonomy in DoD Systems' (Task Force Report, US Department of Defense, July 2012)

Department of Defense, 'Autonomy Research Pilot Initiative (ARPI)' (Invitation for Proposals, November 2012) 1 <http://auvac.org/uploads/publication_pdf/Autonomy%20Research%20Pilot%20Initiati ve.pdf>

Dotterway, Kristen A, Systematic Analysis of Complex Dynamic Systems: The Case of the USS Vincennes (Masters Thesis, Naval Postgraduate School, 1992) <http://www.dtic.mil/get-tr-doc/pdf?AD=ADA260260>

Ecuador, Naval Manual (1989) Aspectos Importantes del Derecho Internacional Marítimo que Deben Tener Presente los Comandantes de los Buques, Academia de Guerra Naval, 1989

Fogarty, William, 'Formal Investigation into the Circumstances Surrounding the Downing of Iran Air Flight 655 on 3 July 1988' (Investigation Report, 19 August 1988) <http://www.dod.mil/pubs/foi/Reading_Room/International_Security_Affairs/172.pdf>

France, LOAC Manual (2001) Manuel de droit des conflits armés, Ministère de la Défense, Direction des Affaires Juridiques, Sous-Direction du droit international humanitaire et du droit européen, Bureau du droit des conflits armés, 2001.

Humanitarian Law in Armed Conflicts – Manual, DSK VV207320067, edited by The Federal Ministry of Defence of the Federal Republic of Germany, VR II 3, August 1992, English

translation of ZDv 15/2, Humanitäres Völkerrecht in bewaffneten Konflikten – Handbuch, August 1992. This manual was superseded by Law of Armed Conflict - Manual, Joint Service Regulation (ZDv) 15/2, DSK AV230100262, Federal Ministry of Defence, Berlin, 1 May 2013, English version of ZDv 15/2, Humanitäres Völkerrecht in bewaffneten Konflikten - Handbuch, 1 May 2013.

Legal Review of New Weapons, Australian Department of Defence Instruction (General) OPS 44-1, 2 June 2005.

Lin, Patrick, George Bekey, and Keith Abney, 'Autonomous Military Robotics: Risk, Ethics, and Design' (Report No ADA534697, US Department of Navy, Office of Naval Research, 20 December 2008) <http://www.dtic.mil/cgibin/GetTRDoc?AD=ADA534697>

Manual for Military Commissions, published in implementation of Chapter 47A of Title 10, United States Code, as amended by the Military Commissions Act of 2009, 10 U.S.C, §§ 948a, *et seq*., 27 April 2010.

McKenna, Tim et al., 'Science & Technology for Australian Network-Centric Warfare: Function, Form and Fit' (Australian Government Department of Defence, 2005) <http://docsfiles.com/view.php?view=http://www.dsto.defence.gov.au/attachments/ST%20for%20Australian%20NCW.pdf&keyword=the%20australian%20approach%20to%20warfare&count=>

Military Manual (1992) Interim Law of Armed Conflict Manual, DM 112, New Zealand Defence Force, Headquarters, Directorate of Legal Services, Wellington, November 1992.

Ministry of Defence, 'The UK Approach to Unmanned Aircraft Systems' (Joint Doctrine Note 2/11, 30 March 2011)

National Defense and the Canadian Armed Forces, *Chapter 1: The Purpose of Military Justice*, Government of Canada (2017), available at <www.forces.gc.ca/en/about-reports-pubs-military-law-summary-trial-level/ch-1-purpose-of-mil-justice.page>

NATO. 2010. *AJP-01D Allied Joint Doctrine*, North Atlantic Treaty Organization, 21 December. Available online at <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33694/AJP01D.pdf>

Nelson, William, 'Use of Circular Error Probability in Target Detection' (Technical Report, MITRE Corporation, May 1988) <http://www.dtic.mil/dtic/tr/fulltext/u2/a199190.pdf>

Norway: *Direktiv om folkerettslig vurdering av vapen, krigforingsmetoder og krigforingsvirkemidler*, (Directive on the Legal Review on Weapons, Methods and Means of Warfare), Ministry of Defence, 18 June 2013.

Office of the Secretary of Defense, 'Unmanned Aircraft Systems Roadmap, 2005 – 2030' (US Department of Defense, 4 August 2005) <https://fas.org/irp/program/collect/uav_roadmap2005.pdf>

Ordonnance du Département fédéral de la défense, de la protection de la population et des sports (DDPS) sur le matériel de l'armée (OMat) [Ordinance of the Swiss Federal Department of Defence, Civil Protection and Sport (DDPS) on the equipment of the armed forces], Law no. 514.20, 6 Dec. 2007; and Weisungen über das Armee material (WAMAT) [Directive on the equipment of the armed forces], 4 Mar. 2009, <https://www.vtg.admin.ch/internet/vtg/de/home/themen/zsham>.

Proud, Ryan W, Jeremy J Hart and Richard B Mrozinski, 'Methods for Determining the Level of Autonomy to Design into a Human Spaceflight Vehicle: A Function Specific Approach' (Report, NASA Johnson Space Center, September 2003) 4 <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA515467>

Secretary of Defense, 'DoD Policy on Cluster Munitions and Unintended Harm to Civilians' (Memorandum, United States Department of Defense, 19 June 2008) <http://www.acq.osd.mil/tc/treaties/ccwapl/DoD%20Policy%20on%20Cluster%20Munitions.pdf>

Strategic Technology Office, Defense Advanced Research Projects Agency, 'Military Imaging and Surveillance Technology — Long Range (MIST-LR) Phase 2' (Broad Agency Announcement No DARPA-BAA-13-27, 12 March 2013) <https://www.fbo.gov/index?s=opportunity&mode=form&id=78b0ddbf382678fa9ace985380108f89&tab=core&_cview=0>

Sweden: *Förordning om folkrättslig granskning av vapenproject* (Ordinance on international law review of arms projects), Swedish Code of Statutes, SFS2007:936.

Tank-Automotive Research, Development, and Engineering Center, 'Robotics Strategy White Paper' (Army Capabilities Integration Center, US Army, 19 March 2009) (http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA496734>

The 1978 Directive of the Minister of Defence (nr. 458.614/A) establishing the Committee for International Law and the Use of Conventional Weapons. (Beschikking van de Minister van Defensie, Adviescommissie Internationaal Recht en Conventioneel Wapengebruik).

The 2003 Norway Ministry of Defence Directive on the Legal Review on Weapons, Methods and Means of Warfare (Direktiv om folkerettslig vurdering av vapen, krigforingsmetoder og krigforingsvirkemidler)

The 2005 Australian Department of Defence Instruction on Legal Review of New Weapons (OPS 44-1).

The Belgian 2002 Committee for the Legal Review of New Weapons, New Means and New Methods of Warfare (La Commission d'Evaluation Juridique des nouvelles armes, des nouveaux moyens et des nouvelles méthodes de guerre. Défense, Etat-Major de la Défense, Ordre Général - J/836).

The Manual of Armed Forces Law (Second Edition) Volume 4 '*Law of Armed Conflict*' Defence Force Order Chapter 7, Section 4 <http://www.nzdf.mil.nz/downloads/pdf/public-docs/> accessed on 29 March 2018.

The Netherlands: *Beschikking van de Minister van Defensie* (Directive of the Minister of Defence) nr. 458.614/A, 5 May 1978, establishing the *Adviescommissie Internationaal Recht en Conventioneel Wapengebruik* (Committee for International Law and the Use of Conventional Weapons).

The Swedish Ordinance on International Law Review of Arms Projects, Swedish Code of Statutes, SFS 1994:536. (Förordning om folkrättslig granskning av vapenproject).

The United States: Review of Legality of Weapons under International Law, US Department of Defense Instruction 5500.15, 16 October 1974

UK Ministry of Defence Development Concepts and Doctrine Centre, UK Weapon Reviews (2016) <https://www.gov.uk/government/publications/uk-weapon-reviews>.

United States Air Force, 'United States Air Force Unmanned Aircraft Systems Flight Plan, 2009-2047' (Report No ADA505168, Headquarters, United States Air Force, 18 May 2009) <http://www.dtic.mil/cgibin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA505168>

United States, Executive Order 13440, 'Interpretation of the Geneva Conventions Common Article 3 as Applied to a Program of Detention and Interrogation Operated by the Central Intelligence Agency', 20 July 2007; available at <http://www.archives.gov/federal-register/executive-orders/2007.html>

United States, The Commander's Handbook on the Law of Naval Operations, NWP 1-14M/MCWP 5-12.1/COMDTPUB P5800.7, issued by the Department of the Navy, Office of the Chief of Naval Operations and Headquarters, US Marine Corps, and Department of Homeland Security, US Coast Guard, July 2007, § 8.1

US Army Science Board, 'Ad-hoc Study on Human Robot Interface Issues' (September 2002) 16 <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA411834>

US Department of Defense, 'Autonomy in Weapon Systems' (Directive No 3000.09, Office of the Under Secretary of Defense for Policy, 21 November 2012)

US Department of Defense, 'Unmanned Systems Integrated Roadmap FY2011-2036' (No 11-S-3613)

USA, Air Force Commander's Handbook (1980) Air Force Pamphlet 110-34, Commander's Handbook on the Law of Armed Conflict, Judge Advocate General, US Department of the Air Force, 25 July 1980.

USA, Air Force Pamphlet (1976) Air Force Pamphlet 110-31, International Law – The Conduct of Armed Conflict and Air Operations, US Department of the Air Force, 1976.

Cases

'Case No 57: The I G Farben Trial: Trial of Carl Krauch and Twenty-Two Others (United States Military Tribunal, Nuremberg)' in United Nations War Crimes Commission, Law Reports of Trials of War Criminals (His Majesty's Stationery Office, 1949) vol 10, 5

'Case No 9: The Zyklon B Case: Trial of Bruno Tesch and Two Others (British Military Court, Hamburg)' in United Nations War Crimes Commission, Law Reports of Trials of War Criminals (His Majesty's Stationery Office, 1947) vol 1, 93

Abdelfattah v. U.S. Department of Homeland Security, 893 F.Supp.2d 75, 76 n. 2 (D.D.C.2012)
Decision on the Confirmation of Charges, *Prosecutor v Katanga (Trial Judgment)* (International Criminal Court, Pre-Trial Chamber I, Case No ICC-01/04-01/07-717, 30 September 2008)

Decision on the Confirmation of Charges, *Situation in the Democratic Republic of the Congo, in the case of the Prosecutor v. Thomas Lubanga Dyilo* (International Criminal Court, Pre-Trial Chamber I, Case No ICC-01/04-01/06-803, 29 January 2007)

Decision Pursuant to Art 61(7)(a) and (b) of the Rome Statute on the Charges of the Prosecutor against Jean-Pierre Bemba Gombo, *Bemba* (International Criminal Court, Pre-Trial Chamber II, Case No ICC-01/05-01/08-424, 15 June 2009)

Eritrea-Ethiopia Claims Commission, Partial Award, Western Front, Aerial Bombardment and Related Claims, Eritrea's Claims 1, 3, 5, 9-13, 14, 21, 25 and 26 (19 December 2005), Report of International Arbitration Awards, vol XXVI, 291-349

Hassan v. the United Kingdom, 29750/09, Council of Europe: European Court of Human Rights, Grand Chamber, Judgment, 16 September 2014

Inter-American Commission on Human Rights *Case 11.137 (Argentina)* Argentina, Case 11.137,

International Court of Justice, 'Advisory Opinion - Difference Relating to Immunity from Legal Process of a Special Rapporteur to the Commission of Human Rights', (1999) ICJ Reports, 62

International Court of Justice, 'Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)', (2005) ICJ Reports, 168

International Court of Justice, 'Case Concerning the Application of the Convention of the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) (Merits)', (2007) ICJ Reports, 43

International Court of Justice, 'Corfu Channel (United Kingdom v. Albania)', (1949) ICJ Reports, 4

International Court of Justice, Fisheries Jurisdiction (Spain v Canada) (Judgment) (1998) ICJ Reports, 432

International Court of Justice, Gabčíkovo-Nagyamaros Project (Hungary v Slovakia) (Judgment), (1997) ICJ Reports, 7

International Court of Justice, Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) (1996) ICJ Reports, 226

International Court of Justice, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, (1986) ICJ Reports, 101

Ireland v. The United Kingdom, 5310/71, Council of Europe: European Court of Human Rights, 13 December 1977

Juan Carlos Abella, Report 55/97 of 18 November 1997, IACiHR Annual Report 1997, Doc. OEA/Ser.L/V/II.98, Doc. 7 rev., 13 April 1998, 271

Jurisdictional Immunities of the State (Germany v. Italy: Greece Intervening), Judgment, T 64 (Feb. 3, 2012)

Katz v United States 389 US 347

Latif v. Holder, 28 F.Supp.3d 1134 (D.Or.2014)

Noble Ventures Inc v Romania (Award) (ICSID Arbitral Tribunal, Case No ARB/01/11, 12 October 2005)

Olmstead v United States 277 US 438, 466 (1928)

Prosecutor v Aleksovski (Judgement), (International Criminal Tribunal for the former Yugoslavia, Case No IT-95-14/1-T, 25 June 1999)

Prosecutor v Bemba Gombo (Judgment) (International Criminal Court, Trial Chamber III, Case No ICC-01/05-01/08, 21 March 2016)

Prosecutor v Blaškić (Appeal Judgement) (International Criminal Tribunal for the Former Yugoslavia, Appeals Chamber, Case No IT-95-14-A, 29 July 2004)

Prosecutor v Chui (Judgment Pursuant to Article 74 of the Statute) (International Criminal Court, Trial Chamber II, Case No ICC-01/04–02/12, 18 December 2012)

Prosecutor v Furundžija (Judgement) (International Criminal Tribunal for the Former Yugoslavia, Trial Chamber, Case No IT-95-17/1-T, 10 December 1998)

Prosecutor v Katanga (Trial Judgment) (International Criminal Court, Trial Chamber II, Case No ICC-01/04-01/07, 7 March 2014)

Prosecutor v Kordić (Appeal Judgement) (International Criminal Tribunal for the Former Yugoslavia, Appeals Chamber, Case No IT-95-14/2-A, 17 December 2004)

Prosecutor v Kupreškić (Judgement) (International Criminal Tribunal for the Former Yugoslavia, Trial Chamber, Case No IT-95-16, 14 January 2000)

Prosecutor v Mucić (Judgement) (International Criminal Tribunal for the Former Yugoslavia, Trial Chamber, Case No IT-96-21-T, 16 November 1998)

Prosecutor v Nikolić (Decision on Defence Motion Challenging the Exercise of Jurisdiction by the Tribunal) (International Criminal Tribunal for the Former Yugoslavia, Trial Chamber II, Case No IT–94–2–PT, 9 October 2002)

Prosecutor v Strugar (Judgement) (International Criminal Tribunal for the Former Yugoslavia, Appeals Chamber, Case No IT-01-42-A, 17 July 2008)

Prosecutor v Strugar (Trial Judgement) (International Criminal Tribunal for the Former Yugoslavia, Trial Chamber II, Case No IT-01-42-T, 31 January 2005)

Prosecutor v Tadić (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction) (International Criminal Tribunal for the Former Yugoslavia, Appeals Chamber, Case No IT-94-1-1, 2 October 1995)

Prosecutor v Taylor (Judgement) (Special Court for Sierra Leone, Trial Chamber II, Case No SCSL-03-01-T, 18 May 2012)

Prosecutor v. Dragoljub Kunarac, Radomir Kovac and Zoran Vukovic (Trial Judgment), (International Criminal Tribunal for the former Yugoslavia, Trial Chamber, Case No IT-96-23-T & IT-96-23/1-T, 22 February 2001)

Prosecutor v. Halilovic (Appeal Judgment) (International Criminal Tribunal for the former Yugoslavia, Appeals Chamber, Case No IT-01-48-A, 16 October 2007)

Prosecutor v. Halilovic (Trial Judgment) (International Criminal Tribunal for the former Yugoslavia, Trial Chamber, Case No IT-01-48-T, 16 November 2005)

Prosecutor v. Haradinaj et al. (Trial Judgment) (International Criminal Tribunal for the former Yugoslavia, Trial Chamber, Case No IT-04-84-T, 3 April 2008)

Prosecutor v. Kupreskic et al. (Trial Judgement), (International Criminal Tribunal for the former Yugoslavia, Trial Chamber, Case No IT-95-16-T, 14 January 2000)

Prosecutor v. Mladen Naletilic aka "Tuta", Vinko Martinovic aka "Stela" (Appeal Judgement), (International Criminal Tribunal for the former Yugoslavia, Appeals Chamber, Case No IT-98-34-A, 3 May 2006)

Prosecutor v. Naser Oric (Trial Judgment) (International Criminal Tribunal for the former Yugoslavia, Trial Chamber, Case No IT-03-68-T, 30 June 2006)

Prosecutor v. Rodovan Karadzic (Decision on Karadzic's Appeal of the Trial Chamber's Decision on Alleged Holbrooke Agreement), (International Criminal Tribunal for the former Yugoslavia, Appeals Chamber, Case No IT-95-5/18-AR73.4, 12 October 2009)

Prosecutor v. Ruto, Kosgey and Sang, (International Criminal Court, Pre-Trial Chamber II, Case No ICC-01/ 09-01/11, 23 January 2012)

Prosecutor v. Stanilav Galic (Trial Judgement and Opinion) (International Criminal Tribunal for the former Yugoslavia, Trial Chamber, Case No IT-98-29-T, 5 December 2003)

Prosecutor v. Stanislav Galić, (Judgement), (International Criminal Tribunal for the former Yugoslavia, Trial Chamber, Case No ICTY-98-23-T, 5 Dec 2003)

Prosecutor v. Tihomir Blaskic (Judgement), (International Criminal Tribunal for the former Yugoslavia, Appeals Chamber, Case No IT-95-14/A, 29 July 2004)

Prosecutor v. Tihomir Blaskic (Trial Judgement), (International Criminal Tribunal for the former Yugoslavia, Case No 3 IT-95-14-T, 3 March 2000)

Prosecutor v. Zdravko Mucic aka "Pavo", Hazim Delic, Esad Landzo aka "Zenga", Zejnil Delalic (Trial Judgement), (International Criminal Tribunal for the former Yugoslavia, Trial Chamber, Case No IT-96-21-T, 16 November 1998)

Prosecutor v. Zdravko Mucic aka "Pavo", Hazim Delic, Esad Landzo aka "Zenga", Zejnil Delalic (Appeal Judgement), (International Criminal Tribunal for the former Yugoslavia, Appeals Chamber, Case No IT-96-21-A, 20 February 2001)

Public Committee Against Torture in Israel v. Israel, (2007) 46 I.L.M. 375 (Supreme Court of Israel sitting as the High Court of Justice, 16 December 2006) [PCATI]

Selmouni v. France, 25803/94, Council of Europe: European Court of Human Rights, 28 July 1999

Situation in the Democratic Republic of the Congo, in the case of the Prosecutor v. Thomas Lubanga Dyilo, (International Criminal Court, Case No ICC-01/04-01/06, 14 March 2012)

Supreme Court of Israel, *Iyad v. State of Israel*, [1] CrimA 6659/06, 11 June 2008, available at <http://elyon1.court.gov.il/files-eng/06/590/066/n04/06066590.n04.pdf>

The Prosecutor v. Ferdinand Nahimana, Jean-Bosco Barayagwiza, Hassan Ngeze (Appeal Judgment) (International Criminal Tribunal for Rwanda, Appeals Chamber, Case No ICTR-99-52-A, 28 November 2007)

The Prosecutor v. Gotovina et al. (Judgment) - Vol. 2, (International Criminal Tribunal for the former Yugoslavia, Trial Chamber, Case No IT-06-90-A, 16 November 2012)

The Prosecutor v. Jean-Paul Akayesu (Trial Judgement), (International Criminal Tribunal for Rwanda, Trial Chamber, Case No ICTR-96-4-T, 2 September 1998)

The Prosecutor v. Milutinovic et al. (Judgment) (International Criminal Tribunal for the former Yugoslavia, Case No IT-99-37-AR72, 21 May 2003)

The United States of America v Carl Krauch, et al,

Trail Smelter Arbitration (United States v. Canada) Arbitral Tribunal, 3 U.N. Rep. International Arbitration Awards 1905 (1941)

Tyrer v. The United Kingdom, 5856/72, Council of Europe: European Court of Human Rights, 15 March 1978

UN Security Council, *Security Council resolution 1329 (2000) [on the International Criminal Tribunal for the former Yugoslavia and International Criminal Tribunal for Rwanda]*, 5 December 2000, S/RES/1329 (2000)

Xuncax v. Gramajo, 886 F. Supp. 162, 183 (D. Mass. 1995)

Legislation

Alien Tort Statute, 28 USC § 135 (2012)

National Prohibition Act 41 Stat 305, ch 85

Treaties

'Declaration IV, 1 to Prohibit for the Term of Five Years the Launching of Projectiles and Explosives from Balloons, and Other New Methods of a Similar Nature' in James Scott Brown (ed), *The Hague Conventions and Declarations of 1899 and 1907* (Oxford University Press, 2nd ed, 1915) 220

'Declaration IV, 2 Concerning Asphyxiating Gases' in James Scott Brown (ed), *The Hague Conventions and Declarations of 1899 and 1907* (Oxford University Press, 2nd ed, 1915) 225

'Declaration IV, 3 Concerning Expanding Bullets' in James Scott Brown (ed), *The Hague Conventions and Declarations of 1899 and 1907* (Oxford University Press, 2nd ed, 1915) 227

‘Declaration XIV Prohibiting the Discharge of Projectiles and Explosives from Balloons’ in James Scott Brown (ed), *The Hague Conventions and Declarations of 1899 and 1907* (Oxford University Press, 2nd ed, 1915) 220

Additional Protocol to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to have Indiscriminate Effects (Protocol IV, entitled Protocol on Blinding Laser Weapons), opened for signature 13 October 1995, 2024 UNTS 163 (entered into force 30 July 1998)

Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, signed 18 October 1907, 205 CTS 299 (entered into force 26 January 1910)

Convention for the Amelioration of the Condition of the Wounded in Armies in the Field, opened for signature 22 August 1864, 22 Stat 940 (entered into force 22 June 1865)

Convention on Cluster Munitions, opened for signature 30 May 2008, 2688 UNTS 39 (entered into force 1 August 2010)

Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, opened for signature 10 October 1980, 1342 UNTS 137 (entered into force 2 December 1983)

Convention on the Prevention and Punishment of the Crime of Genocide, opened for signature 9 December 1948, 78 UNTS 277 (entered into force 12 January 1951)

Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, opened for signature 10 April 1972, 1015 UNTS 163 (entered into force 26 March 1975)

Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, opened for signature 13 January 1993, 1974 UNTS 45 (entered into force 29 April 1997)

Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti Personnel Mines and on their Destruction, opened for signature 18 September 1997, 2056 UNTS 211 (entered into force 1 March 1999)

Convention respecting the Laws and Customs of War on Land and its Annex: Regulations concerning the Laws and Customs of War on Land, signed 18 October 1907 [1910] ATS 8 (entered into force 26 January 1910)

Declaration Renouncing the Use, in Time of War, of Explosive Projectiles under 400 Grams Weight, [1901] ATS 125 (signed and entered into force 11 December 1868)

Draft Rules for the Limitation of the Dangers Incurred by the Civilian Population in Time of War (International Committee of the Red Cross, 1956) <https://www.icrc.org/ihl/INTRO/420?OpenDocument>

Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, opened for signature 12 August 1949, 75 UNTS 31 (entered into force 21 October 1950)

Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, opened for signature 12 August 1949, 75 UNTS 85 (entered into force 21 October 1950)

Geneva Convention Relative to the Protection of Civilian Persons in Time of War, opened for signature 12 August 1949, 75 UNTS 287 (entered into force 21 October 1950)

Geneva Convention Relative to the Treatment of Prisoners of War, opened for signature 12 August 1949, 75 UNTS 135 (entered into force 21 October 1950)

International Convention for Adapting to Maritime Warfare the Principles of the Geneva Convention of 22 August 1864, signed 29 July 1899, [1901] ATS 132 (entered into force 4 September 1900)

International Convention for the Pacific Settlement of International Disputes, signed 29 July 1899, [1901] ATS 130 (entered into force 4 September 1900)

International Convention relative to the Laying of Automatic Submarine Contact Mines, signed 18 October 1907, [1910] ATS 11 (entered into force 26 January 1910)

International Convention with respect to the Laws and Customs of War on Land, signed 29 July 1899, [1901] ATS 131 (entered into force 4 September 1900)

International Covenant on Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976)

Project of an International Declaration concerning the Laws and Customs of War, signed 27 August 1874 (reprinted in: *The Proceedings of the Hague Peace Conferences: The Conference of 1899* (James Brown Scott trans, William S Hein & Co, 2000) 564 [trans of: *Conférence internationale de la paix. La Haye*, 18 mai-29 juillet 1899. (first published 1907)])

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), opened for signature 8 June 1977, 1125 UNTS 3 (entered into force 7 December 1978)

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), opened for signature 8 June 1977, 1125 UNTS 609 (entered into force 7 December 1979)

Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or other Gases, and of Bacteriological Methods of Warfare, opened for signature 17 June 1925, [1930] ATS 6 (entered into force 8 February 1928)

Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices as amended on 3 May 1996 (Protocol II, as amended on 3 May 1996) annexed to the Convention on

Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to have Indiscriminate Effects, opened for signature 3 May 1996, 2048 UNTS 93 (entered into force 3 December 1998)

Rome Statute of the International Criminal Court, opened for signature 17 July 1998, 2187 UNTS 90 (entered into force 1 July 2002)

The Laws of War on Land: Manual Published by the Institute of International Law, adopted 9 September 1880 (reprinted in: *Resolutions of the Institute of International Law Dealing with the Law of Nations* (James Brown Scott trans, William S Hein & Co, 2003)

UN General Assembly, *United Nations Convention on Jurisdictional Immunities of States and Their Property*, 2 December 2004, A/RES/59/38

United Nations Documents

Alston, Philip, *Interim Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions*, UN GAOR, 65th sess, Agenda Item 69(b), UN Doc A/65/321 (23 August 2010)

Final Report of the Meeting of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, 2013 sess, Agenda Item 13, UN Doc CCW/MSP/2013/10 (16 December 2013)

Heyns, Christof, *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Human Rights Council*, 23rd sess, Agenda Item 3, UN Doc A/HRC/23/47 (9 April 2013)

Heyns, Christof, *Statement by Mr Christof Heyns, Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions*, UN GAOR, 3rd Comm, 65th sess, Agenda Item 68(a) (22 October 2010)

Materials on the Responsibility of States for Internationally Wrongful Acts, United Nations Legislative Series Book 25, UN Doc ST/LEG/SER.B/25, (2012)

Recommendations to the 2016 Review Conference 1 <http://www.unog.ch/80256EDD006B8954/(httpAssets)/6BB8A498B0A12A03C1257FDB00382863/$file/Recommendations_LAWS_2016_AdvancedVersion+(4+paras)+.pdf>

Report of the 2014 Informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), 2014 sess, Provisional Agenda Item 8, UN Doc CCW/MSP/2014/3 (11 June 2014)

Report of the 2015 Informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), 2015 sess, Provisional Agenda Item 8, UN Doc CCW/MSP/2015/3 (2 June 2015)

Report of the 2016 Informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS) (Advanced Version) <http://www.unog.ch/80256EDD006B8954/(httpAssets)/DDC13B243BA863E6C1257FDB00380A88/$file/ReportLAWS_2016_AdvancedVersion.pdf>

Report of the International Commission of Inquiry on Darfur to the U.N. Secretary General, 558 (25 January 2005)

Report of the International Law Commission, UN GAOR, 56th sess, Supp No 10, UN Doc A/56/10 (2001)

Responsibility of States for Internationally Wrongful Acts, UN GAOR, 6th Comm, 56th sess, 85th plen mtg, Agenda Item 162, UN Doc A/RES/56/83 (12 December 2001)

Responsibility of States for Internationally Wrongful Acts, UN GAOR, 6th Comm, 59th sess, 65th plen mtg, Agenda Item 139, UN Doc A/RES/59/35 (2 December 2004)

Responsibility of States for Internationally Wrongful Acts, UN GAOR, 6th Comm, 62nd sess, 62nd plen mtg, Agenda Item 78, UN Doc A/RES/62/61 of 6 December 2007

Responsibility of States for Internationally Wrongful Acts, UN GAOR, 6th Comm, 65th sess, 57th plen mtg, Agenda Item 75, UN Doc A/RES/65/19 (6 December 2010)

Work of the Advisory Board on Disarmament Matters: Report of the Secretary-General, UN GAOR, 68th sess, Provisional Agenda Item 101, UN Doc A/68/206 (26 July 2013)

Websites

'Kunduz Bombing: German Court Drops Case over Civilian Deaths' (*Spiegel Online International*, 11 December 2013) Available online at <http://www.spiegel.de/international/germany/court-says-germany-not-responsible-for-damages-in-afghanistan-attack-a-938490.html>

Ackerman, Spencer, 'Here´s How Darpa´s Robot Ship Will Hunt Silent Subs' (27 December 2012) available online <https://www.wired.com/2012/12/actuv/>

Adams, William Lee, *Brief History: Wiretapping* (11 October 2010) Time Magazine <http://content.time.com/time/magazine/article/0,9171,2022653,00.html>

Advanced Medium Range Air-to-Air Missile (AMRAAM), Naval Air Systems Command <http://www.navair.navy.mil/index.cfm?fuseaction=home.display&key=D3FAC4AB2E9F-4150-9664-6AFBC83F203E>

Aegis Combat System, Lockheed Martin <http://www.lockheedmartin.com.au/us/products/aegis.html>

Bolton, Matthew, Thomas Nash and Richard Moyes, *Ban Autonomous Armed Robots* (5 March 2012) Article 36 <http://www.article36.org/statements/ban-autonomous-armedrobots/>

Burridge, Brian, *U.K. Inquiry into Iraq ('Chilcot Inquiry')* (2009) Available online at <http://www.iraqinquiry.org.uk/media/39393/091208burridge-brims.pdf>

Crawford, James, *Articles on Responsibility of States for Internationally Wrongful Acts: Historical Background and Development of Codification*, United Nations Audiovisual Library of International Law <http://legal.un.org/avl/ha/rsiwa/rsiwa.html>

DARPA Tactical Technology Office, Defense Advanced Research Projects Agency, Hydra <http://www.darpa.mil/Our_Work/TTO/Programs/Hydra.aspx>

Defence Science and Technology Organisation, *Network-Centric Warfare* (3 September 2007) Australian Government Department of Defence <http://www.dsto.defence.gov.au/research/4051/>

Federal Business Opportunities, Hydra (22 August 2013) <https://www.fbo.gov/index?s=opportunity&mode=form&id=4cc32f06144bd6f3eba18655135d6155&tab=core&_cview=1>

Federal Research Division, *Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts* (16 July 2010) Library of Congress <https://www.loc.gov/rr/frd/Military_Law/RC-dipl-conference-records.html>

Fiddian, Peter, 'UAV Swarm Technology Trial Success' (*Armed Forces International News,* 13 March 2012). Available online at <http://www.armedforces-int.com/news/uav-swarm-technology-trial-success.html>

First Committee, *Disarmament and International Security - Documents of the 68th Session*, General Assembly of the United Nations <http://www.un.org/en/ga/first/68/documentation.shtml>

France convenes Seminar at the UN (26 September 2013) Campaign to Stop Killer Robots <http://www.stopkillerrobots.org/2013/09/france-seminar/>

Glanz, James & Andrew Lehren, 'Use of Contractors Added to War's Chaos in Iraq' (*The New York Times,* 23 October 2010) <www.nytimes.com/2010/10/24/world/middleeast/24contractors.html?_r=2&hp&>

Global Patriot Solutions, Raytheon <http://www.raytheon.com/capabilities/products/patriot/>

Harpy Air Defense Suppression System (4 March 2006) Defense Update: International Online Defense Magazine <http://defense-update.com/directory/harpy.htm>

Harpy NG, Israel Aerospace Industries <http://www.iai.co.il/2013/36694-16153en/IAI.aspx>

Hartshorn, Derick S, Mk 60 (Captor) (28 November 2009) Mineman Memories <http://www.hartshorn.us/Navy/navy-mines-10.htm>

International Committee of the Red Cross, 'Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centered Approach' (6 June 2019) <https://www.icrc.org/en/document/artificial-intelligenceand-machine-learning-armed-conflict-human-centred-approach>

Iron Dome Weapon System, Raytheon <http://www.raytheon.com/capabilities/products/irondome/>

Jackson, Richard, 'Remarks in Panel on Autonomous Weaponry and Armed Conflict' Annual Meeting of American Society of International Law, 10 April 2014. Video available online at <https://www.youtube.com/watch?v=duq3DtFJtWg&list=PLYp0ZUypbrnevQlBfMUSDG0IanrvJ3J6z&index=4>

Joint Strike Missile (JSM) Brochure, Kongsberg <https://www.kongsberg.com/~/media/KDS/Files/Products/Missiles/jsm_web_reduced. ashx>

Keller, John, *DARPA Considers Unmanned Submersible Mothership Designed to Deploy UAVs and UUVs* (23 July 2013) Military & Aerospace Electronics <http://www.militaryaerospace.com/articles/2013/07/darpa-uuv-mothership.html>

Kumagai, Jean, *A Robotic Sentry for Korea's Demilitarized Zone* (1 March 2007) IEEE Spectrum <http://spectrum.ieee.org/robotics/military-robots/a-robotic-sentry-for-koreasdemilitarized-zone>

Lawlor, Maryann, 'Combat-Survivable Unmanned Aircraft Take Flight' (2003) available online <http://www.afcea.org/content/?q=combat-survivable-unmanned-aircraft-take-flight>

Lockheed Martin Corporation, *K-MAX* <http://www.lockheedmartin.com/us/products/kmax.html>

Markoff, John, 'Fearing Bombs That Can Pick Whom to Kill' (*The New York Times*, 11 Nov 2014) <https://www.nytimes.com/2014/11/12/science/weapons-directed-by-robots-not-humans-raise-ethical-questions.html>

Markoff, John, 'Old Trick Threatens New Weapons' (*The New York Times*, 26 October 2009). Available online at <http://www.nytimes.com/2009/10/27/science/27trojan.html?pagewanted=all&_r=0>

Meier, Michael, 'U.S. Delegation Statement on "Appropriate Levels of Human Judgment"' (Statement to the CCW Informal Meeting of Experts on AWS, 12 April 2016) <https://geneva.usmission.gov/2016/04/12/u-s-delegation-statement-onappropriate-levels-of-human-judgment/>

Micro Autonomous Systems and Technology (MAST), *Research Thrusts* <https://alliance.seas.upenn.edu/~mastwiki/wiki/index.php?n=Main.Objectives>

Modirzadeh, Naz, Remarks in panel on Autonomous Weaponry and Armed Conflict Annual Meeting of American Society of International Law, 10 April 2014. Video available online at <https://www.youtube.com/watch?v=duq3DtFJtWg&list=PLYp0ZUypbrnevQlBfMUSDG0IanrvJ3J6z&index=4>

NATO Network Enabled Capability (27 October 2010) North Atlantic Treaty Organization <http://www.nato.int/cps/de/SID-815535E457782C82/natolive/topics_54644.htm>

Office of Naval Research, *Autonomous Aerial Cargo/Utility System Program* (27 September 2013) <http://www.onr.navy.mil/en/Science-Technology/Departments/Code35/All-Programs/aerospace-research-351/Autonomous-Aerial-Cargo-UtilityAACUS.aspx>

Phalanx Close-In Weapon System: Last Line of Defense for Air, Land and Sea, Raytheon Australia <http://www.raytheon.com.au/capabilities/products/phalanx/>

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I), United Nations Treaty Collection <https://treaties.un.org/Pages/showDetails.aspx?objid=08000002800f3586>

Sauer, Frank, *Banning Lethal Autonomous Weapon Systems (LAWS): The Way Forward* (13 June 2014) International Committee for Robot Arms Control <http://icrac.net/2014/06/banning-lethal-autonomous-weapon-systems-laws-the-wayforward/>

Sauer, Frank, *ICRAC statement on technical issues to the 2014 UN CCW Expert Meeting* (14 May 2014) International Committee for Robot Arms Control <http://icrac.net/2014/05/icrac-statement-on-technical-issues-to-the-un-ccw-expertmeeting/>
Scharre, Paul, *Between a Roomba and a Terminator: What is Autonomy?* (18 February 2015) War on the Rocks <https://warontherocks.com/2015/02/between-a-roomba-anda-terminator-what-is-autonomy/?singlepage=1>

Shachtman, Noel, *'Army Tracking Plan: Drones That Never Forget a Face'* (28 Sept 2011) <https://www.wired.com/2011/09/drones-never-forget-a-face/>

Singer, Peter, *The Predator Comes Home: A Primer on Domestic Drones, Their Huge Business Opportunities, and Their Deep Political, Moral, and Legal Challenges* (8 March 2013) available at <http://www.brookings.edu/research/papers/2013/03/08-drones-singer>

Tozer, Jessica, *'Robots with Faces, Armed with Science'* (5 April 2012) <http://science.dodlive.mil/2012/04/05/robots-with-faces/>

United States Army Research Laboratory, *Micro Autonomous Systems and Technology (MAST)* (25 February 2011) <http://www.arl.army.mil/www/default.cfm?page=332>

Wallach, Wendell, 'Terminating the Terminator: What to Do About Autonomous Weapons' (29 January 2013) available online <https://scienceprogress.org/2013/01/terminating-the-terminator-what-to-do-aboutautonomous-weapons/>

Other

'Final Act of the International Peace Conference' in James Scott Brown (ed), *The Hague Conventions and Declarations of 1899 and 1907* (Oxford University Press, 2nd ed, 1915) 1

'Final Act of the Second International Peace Conference' in James Scott Brown (ed), *The Hague Conventions and Declarations of 1899 and 1907* (Oxford University Press, 2nd ed, 1915) 1

‘Russian Circular Note Proposing the Program of the First Conference’ in James Scott Brown (ed), *The Hague Conventions and Declarations of 1899 and 1907* (Oxford University Press, 2nd ed, 1915) xvii

Amnesty International (Statement, CCW Meeting of Experts on LAWS: Human Rights and Ethical Issues, April 2016)

Belgium (Presentation, CCW Meeting of Experts on LAWS: Challenges to International Humanitarian Law, April 2016)

Borrie, John (Presentation, CCW Meeting of Experts on LAWS: Security Issues, April 2016)

Bourcier, Daniele (Presentation, CCW Meeting of Experts on LAWS: Human Rights and Ethical Issues, April 2016)

Brehm, Maya (Presentation, CCW Meeting of Experts on LAWS: Characteristics of LAWS, April 2015)

Canada (Opening Statement, CCW Meeting of Experts on LAWS: General Exchange, April 2016)

Center for a New American Security (Opening Statement, CCW Meeting of Experts on LAWS: General Exchange, April 2016)

Center for a New American Security (Text, CCW Meeting of Experts on LAWS: Characteristics of LAWS, April 2015)

Chatila, Raja (Text, CCW Meeting of Experts on LAWS: Technical Issues, May 2014)

Dahlmann, Anja (Presentation, CCW Meeting of Experts on LAWS: Towards a Working Definition of LAWS, April 2016)

France, ‘Characterization of a LAWS’ (Working Paper, CCW Meeting of Experts on LAWS, April 2016)

Galliott, Jai (Presentation, CCW Meeting of Experts on LAWS: Security Issues, April 2016)

General Comment No. 3 on the African Charter on Human and Peoples’ Rights: The Right to Life (Article 4), African Commission on Human and Peoples’ Rights, 57th ordinary session (18 November 2015) 12 [35] <http://www.achpr.org/instruments/general-comments-right-to-life/>

Germany (Opening Statement, CCW Meeting of Experts on LAWS: General Exchange, May 2014)

Germany (Opening Statement, CCW Meeting of Experts on LAWS: General Exchange, April 2016)

Germany (Statement, CCW Meeting of Experts on LAWS: Challenges to International Humanitarian Law, April 2016)

Giacca, Gilles (Notes, CCW Meeting of Experts on LAWS: Challenges to International Humanitarian Law, April 2016)

Harpy NG Anti-Radiation Loitering Weapon System, Israel Aerospace Industries, MBT Missiles Division <http://www.iai.co.il/Sip_Storage//FILES/5/41655.pdf>

Heyns, Christof (Comment, CCW Meeting of Experts on LAWS: Overarching Issues, April 2015)

Heyns, Christof (Note, CCW Meeting of Experts on LAWS: Human Rights and Ethical Issues, April 2016)

Holy See (Text, CCW Meeting of Experts on LAWS: Overarching Issues, April 2015)

Human Rights Watch (Statement, CCW Meeting of Experts on LAWS: Challenges to International Humanitarian Law, April 2016)

International Criminal Court, *Elements of Crimes*, Doc No ICC-ASP/1/3 and Corr.1 and RC/11 (adopted 11 June 2010)

Israel (Opening Statement, CCW Meeting of Experts on LAWS: General Exchange, April 2016)

Israel (Statement, CCW Meeting of Experts on LAWS: Challenges to International Humanitarian Law, April 2016)

Israel (Text, CCW Meeting of Experts on LAWS: Characteristics of LAWS, April 2015)

Japan (Opening Statement, CCW Meeting of Experts on LAWS: General Exchange, April 2016)

Jenks, Chris (Notes, CCW Meeting of Experts on LAWS: Towards a Working Definition of LAWS, April 2016)

Kalmanovitz, Pablo (Notes, CCW Meeting of Experts on LAWS: Human Rights and Ethical Issues, April 2016)

Karnouskos, Stamatis, 'Stuxnet Worm Impact on Industrial Cyber-Physical System Security' (Paper presented at IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society, Melbourne, Victoria, Australia, 7–10 November 2011)

Kester, Leon (Notes, CCW Meeting of Experts on LAWS: Mapping Autonomy, April 2016)

Koh, Collin S L (Note, CCW Meeting of Experts on LAWS: Security Issues, April 2016)

Kozyulin, Vadim (Presentation, CCW Meeting of Experts on LAWS: Security Issues, April 2016)

Lieblich, Eliav (Note, CCW Meeting of Experts on LAWS: Human Rights and Ethical Issues, April 2016)

Lin, Patrick (Text, CCW Meeting of Experts on LAWS: Overarching Issues, April 2015)

Mines Action Canada (Statement, CCW Meeting of Experts on LAWS: Challenges to International Humanitarian Law, April 2016)

Moyes, Richard (Notes, CCW Meeting of Experts on LAWS: Towards a Working Definition of LAWS, April 2016)

Netherlands (Statement, CCW Meeting of Experts on LAWS: Challenges to International Humanitarian Law, April 2016)

Norway (Opening Statement, CCW Meeting of Experts on LAWS: General Exchange, May 2014)

Pakistan (Opening Statement, CCW Meeting of Experts on LAWS: General Exchange, April 2016)

Poland (Text, CCW Meeting of Experts on LAWS: Characteristics of LAWS, April 2015)

Republic of Korea (Opening Statement, CCW Meeting of Experts on LAWS: General Exchange, April 2015)

Richter, Wolfgang, 'Utility and Limitations of the Use of LAWS in Military Operations' (Text, CCW Meeting of Experts on LAWS: Operational and Military Aspects, May 2014)

Rickli, Jean-Marc (Text, CCW Meeting of Experts on LAWS: Overarching Issues, April 2015)

Scharre, Paul (Text, CCW Meeting of Experts on LAWS: Technical Issues, May 2014)

Scholtz, Jean, 'Theory and Evaluation of Human Robot Interactions' (Paper presented at 36th Annual Hawaii International Conference on System Sciences, Hawaii, 6–9 January 2003)

Stojanovic, Milica, 'Underwater Acoustic Communications: Design Considerations on the Physical Layer' (Paper presented at Fifth Annual Conference on Wireless on Demand Network Systems and Services, Garmisch-Partenkirchen, Germany, 23-25 January 2008)

Sweden (Opening Statement, CCW Meeting of Experts on LAWS: General Exchange, May 2014)

Sweden (Statement, CCW Meeting of Experts on LAWS: Challenges to International Humanitarian Law, April 2016)

Switzerland (Statement, CCW Meeting of Experts on LAWS: Challenges to International Humanitarian Law, April 2016)

United Kingdom, Parliamentary Debates, House of Lords, 26 March 2013, Column 958, 3pm (Lord Astor of Hever) <http://www.publications.parliament.uk/pa/ld201213/ldhansrd/text/1303260001.htm#st_14>

Switzerland (Statement, CCW Meeting of Experts on LAWS: Towards a Working Definition of LAWS, April 2016)

United Kingdom (Statement, CCW Meeting of Experts on LAWS: Challenges to International Humanitarian Law, April 2016)

United States (Opening Statement, CCW Meeting of Experts on LAWS: General Exchange, April 2016)

van Bezooijen, B J A, P J M D Essens and A L W Vogelaar, 'Military SelfSynchronization: An Exploration of the Concept' (Paper presented at 11th International Command and Control

Research and Technology Symposium, Cambridge, UK, 26–28 September 2006) <http://www.dodccrp.org/events/11th_ICCRTS/html/papers/065.pdf>

Zawieska, Karolina (Presentation & Text, CCW Meeting of Experts on LAWS: Overarching Issues, April 2015)

Articles / Books / Report

'Country Views on Killer Robots' (Campaign to Stop Killer Robots, 13 December 2016) <http://www.stopkillerrobots.org/wpcontent/uploads/2013/03/KRC_CountryViews_13Dec2016.pdf>

'International Criminal Court: Making the Right Choices – Part V: Recommendations to the Diplomatic Conference' (Position Paper No IOR 40/010/1998, Amnesty International, 30 April 1998)

'Summary Record of the Eleventh Meeting (CDDH/III/SR.11)' in *Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts Geneva (1974–1977)* (1978) vol 14, 85

'The Weaponization of Increasingly Autonomous Technologies: Considering how Meaningful Human Control Might Move the Discussion Forward' (Discussion Paper, United Nations Institute for Disarmament Research (UNIDIR), 2014)

Adams, Thomas K, 'Future Warfare and the Decline of Human Decisionmaking' (2012) (Winter) *Parameters* 57

Akande, Dapo, 'Clearing the Fog of War? The ICRC's Interpretive Guidance on Direct Participation in Hostilities' (EJIL: Talk, 4 June 2009) Available at <https://www.ejiltalk.org/clearing-the-fog-of-war-the-icrcs-interpretive-guidance-on-direct-participation-in-hostilities> accessed 19 February 2020

Akerson, David, 'The Illegality of Offensive Lethal Autonomy' in Dan Saxon (eds), *International Humanitarian Law and the Changing Technology of War* (Martinus Nijhoff Publishers, 2013) 79

Alberts, David S, John J Garstka and Frederick P Stein, *Network Centric Warfare* (Department of Defense Command and Control Research Program, 2nd revised ed, 1999)

Alexander, Larry & Kimberly Ferzan, 'Risking Other People's Riskings' in *Reflections on Crime and Culpability: Problems and Puzzles* (Cambridge University Press, 2018) 17, 60

Alldridge, Peter, 'The Doctrine of Innocent Agency' (1990) 3 *Criminal Law Forum* 45

Allen, Colin & Wendell Wallach, 'Moral Machines: Contradiction in Terms or Abdication of Human Responsibility?' in Patrick Lin and others (eds), *Robot Ethics: The Ethical and Social Implications of Robotics* (MIT Press, 2012) 405

Allen, Craig H, 'The Seabots are Coming Here: Should they be Treated as "Vessels"?' (2012) 65 *The Journal of Navigation* 749

Allenby, Braden R, 'Are New Technologies Undermining the Laws of War?' (2014) 70(1) *Bulletin of the Atomic Scientists* 21

Alston, Philip, 'Lethal Robotic Technologies: The Implications for Human Rights and International Humanitarian Law' (2011) 21(2) *Journal of Law, Information and Science* 35

Alston, Philip, 'The CIA and Targeted Killings Beyond Boarders' (2011) 2 *Harvard National Security Journal* 116

Ambos, Kai, 'General Principles of Criminal Law in the Rome Statute' (1999) 10 *Criminal Law Forum* 22

Amoroso, Daniele and Benedetta Giordano, 'Who Is to Blame for Autonomous Weapons Systems' Misdoings?' in Elena Carpanelli and Nicole Lazzerini (eds), *Use and Misuse of New Technologies* (Springer, 2019) 225

Anderson, Kenneth & Matthew Waxman, 'Law and Ethics for Robot Soldiers' (2012) 32 *American University WCL Research Paper* 18

Anderson, Kenneth and Matthew C Waxman, 'Law and Ethics for Autonomous Weapon Systems: Why a Ban Won't Work and How the Laws of War Can' (Hoover Institution, 9 April 2013)

Anderson, Kenneth, 'Targeted Killing and Drone Warfare: How We Came to Debate whether there is a Legal Geography of War' in Peter Berkowitz (eds), *Future Challenges in National Security and Law*, Hoover Institution (Stanford University 2011)

Anderson, Kenneth, 'The Rise of International Criminal Law: Intended and Unintended Consequences' (2009) 20 *European Journal of International Law* 331

Anderson, Kenneth, Daniel Reisner and Matthew Waxman, 'Adapting the Law of Armed Conflict to Autonomous Weapon Systems' (2014) 90 *International Law Studies* 386

Antsaklis, Panos J, Kevin M Passino and S J Wang, 'An Introduction to Autonomous Control Systems' (1991) 11(4) *IEEE Control Systems* 5

Arimatsu, Louise and Schmitt, Michael 'Attacking 'Islamic State' and the Khorasan Group: Surveying the International Law Landscape' (2014) 53 *Columbia Journal of Transnational Law Bulletin* 1

Arjomandi, Maziar, 'Classification of Unmanned Aerial Vehicles' (2007) course material for Mechanical Engineering 3016, University of Adelaide, Australia

Arkin, Ronald C, 'Governing Lethal Behavior: Embedding Ethics in a Hybrid Deliberative/Reactive Robot Architecture' (Technical Report No GIT-GVU-07-11, Mobile Robot Laboratory, College of Computing, Georgia Institute of Technology, 2007) Arkin,

Arkin, Ronald, 'Lethal Autonomous Systems and the Plight of the Non-combatant' in Ryan Kiggins (eds), *The Political Economy of Robots International Political Economy Series* (Palgrave Macmillan, 2018) 325

Arkin, Ronald, 'The Robot Didn't Do I' (2013) Position Paper for the Workshop on Anticipatory Ethics, Responsibility and Artificial Agents 1

Article 36, 'Key Areas for Debate on Autonomous Weapon Systems' (Memorandum for delegates at the CCW Meeting of Experts on AWS, May 2014) <http://www.article36.org/wp-content/uploads/2014/05/A36-CCW-May-2014.pdf>

Article 36, 'Key Elements of Meaningful Human Control' (Background paper to comments prepared by Richard Moyes, Article 36, for the CCW Meeting of Experts on AWS, April 2016)

Article 36, 'Killer Robots: UK Government Policy on Fully Autonomous Weapons' (Policy Paper, April 2013) <http://www.article36.org/wpcontent/uploads/2013/04/Policy_Paper1.pdf?con=&dom=pscau&src=syndication>

Article 36, 'Structuring Debate on Autonomous Weapon Systems' (Memorandum for delegates to the Convention on Certain Conventional Weapons (CCW), November 2013) <http://www.article36.org/wp-content/uploads/2013/11/Autonomous-weapons-memofor-CCW.pdf>

Asaro, Peter, 'Jus Nascendi, Robotic Weapons and the Martens Clause' in Ryan Calo, Michael Froomkin, Ian Kerr (eds), *Robot Law* (Edward Elgar Publishing, 2016) 367

Asaro, Peter, 'On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-Making' (2012) 94 *International Review of the Red Cross* 687

Aspray, William, 'The Stored Program Concept' (1990) 27(9) *IEEE Spectrum* 51

Bachmann, Sascha, 'Targeted Killings: Contemporary Challenges, Risks and Opportunities' (2013) 18 *Journal of Conflict and Security Law* 30

Backstrom, Alan and Ian Henderson, 'New Capabilities in Warfare: An Overview of Contemporary Technological Developments and the Associated Legal and Engineering Issues in Article 36 Weapons Reviews' (2012) 94 *International Review of the Red Cross* 490

Badar, Mohamed Elewa and Sara Porro, 'Rethinking the Mental Elements in the Jurisprudence of the ICC' in Carsten Stahn (eds), *The Law and Practice of the International Criminal Court* (Oxford University Press, 2015) 665

Badar, Mohamed, 'The Mental Element in The Rome Statute of the International Criminal Court: A Commentary from A Comparative Criminal Law Perspective' (2008) 19 *Criminal Law Forum* 473

Baker, Dennis, *Glanville Williams Textbook of Criminal Law* (Sweet & Maxwell, 2015) 374

Barak, Eitan (ed), *Deadly Metal Rain: The Legality of Flechette Weapons in International Law* (Martinus Nijhoff, 2011)

Bass, Gary J, *Stay the Hand of Vengeance: The Politics of War Crimes Tribunals* (Princeton University Press, 2000)

Beard, Jack M, 'Autonomous Weapons and Human Responsibilities' (2014) 45 *Georgetown Journal of International Law* 617

Beard, Jack, ‘Law and War in the Virtual Era’ (2009) 103 *American Journal of International Law* 434, 449

Beck, Susanne, ‘The Problem of Ascribing Legal Responsibility in the Case of Robotics’ (2016) 31 *AI & Society* 473

Beizer, Boris, *Software Testing Techniques* (Dreamtech, 2003)

Bekey, George A, *Autonomous Robots: From Biological Inspiration to Implementation and Control* (MIT Press, 2005)

Belsky, Adam, Mark Merva & Naomi Roht-Arriaza, ‘Implied Waiver Under the ESIA: A Proposed Exception to Immunity for Violations of Peremptory Norms of International Law’ (1989) 77 *California Law Review* 377, 379

Ben-Gal, Irad, ‘Bayesian Networks’ (2008) *Encyclopedia of Statistics in Quality and Reliability* 1

Bergen, Peter and Katherine Tiedemann, ‘Washington's Phantom War: The Effects of the US Drone Programs in Pakistan’ (2011) 90(4) *Foreign Affairs* 12

Bernaz, Nadia, ‘Corporate Criminal Liability under International Law: The New TV S.A.L. and Akhbar Beirut S.A.L. Cases at the Special Tribunal for Lebanon’ (2015) 13 *Journal of International Criminal Justice* 315

Best, Geoffrey *War and Law Since 1945* (Clarendon Press, 1994) 306

Bhuta, Nehal & Stavros Pantazopoulos, ‘Autonomy and Uncertainty: Increasingly Autonomous Weapons Systems and the International Legal Regulation of Risk’ in Nehal Bhuta, Susanne Beck, Robin Geiβ, Hin Liu, & Claus Kreβ (eds), *Autonomous Weapons Systems: Law, Ethics, Policy* (Cambridge University Press, 2016) 290

Bialek, William, Ilya Nemenman and Naftali Tishby, 'Predictability, Complexity, and Learning' (2001) 13 *Neural Computation* 2409

Bianchi, Andrea, 'Human Rights and the Magic of Jus Cogens' (2008) 19 *The European Journal of International Law* 506

Bieri, Matthias & Marcel Dickow, Lethal 'Autonomous Weapon Systems: Future Challenges' (2014) Center for Security Studies, Analysis in Security Policy 3 available at <http://www.css.ethz.ch/publications/pdfs/CSSAnalyse164-EN.pdf>

Blake, Duncan & Joseph Imburgia, 'Bloodless Weapons? The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining them as Weapons' (2010) 66 *Air Force Law Review* 164

Boas, Gideon, James Bischoff and Natalie Reid, *Forms of Responsibility in International Criminal Law. International Criminal Law Practitioners Library Volume I* (Cambridge University Press, 2007) 139

Bohlander, Michael, *Principles of German Criminal Law* (Hart Publishing, 2009) 153

Bohlander, Michael, *The German Criminal Code: A Modern English Translation* (Hart Publishing, 2008) 48

Bohoslavsky, Juan & Jernej Cernic, *Making Sovereign Financing and Human Rights Work* (Hart Publishing, 2014) 63

Boivin, Alexandra, 'The Legal Regime Applicable to Targeting Military Objectives in the Context of Contemporary Warfare' (Research Paper Series No 2/2006, University Centre for International Humanitarian Law, 2006)

Bolt, Alexander, 'The Use of Autonomous Weapons and the Role of the Legal Advisor' in Dan Saxon (eds), *International Humanitarian Law and the Changing Technology of War* (Martinus Nijhoff, 2013) 132

Bolton, Matthew, 'From Minefields to Minespace: An Archeology of the Changing Architecture of Autonomous Killing in US Army Field Manuals on Landmines, Booby Traps and IEDs' (2015) 46 *Political Geography* 41

Boogard, Jeroen, 'Fighting by the Principles: Principles as a Source of International Humanitarian Law' in Marielle Matthee et al (eds) *Armed Conflict and International Humanitarian Law: In Search for the Human Face* (Asser Press, 2013) 4.

Boothby, Bill, 'And For Such Time As: The Time Dimension to Direct Participation in Hostilities' (2010) 42 *International Law and Politics* 753

Boothby, Bill, 'Autonomous Attack—Opportunity or Spectre?' in Terry Gill, Robin Geiss, Robert Heinsch, Tim McCormack, Christophe Paulussen, Jessica Dorsey (eds), *Yearbook of International Humanitarian Law*, vol 16. (T.M.C. Asser Press, 2015) 73

Boothby, William H, *Conflict Law: The Influence of New Weapons Technology, Human Rights and Emerging Actors* (Asser, 2014)

Boothby, William H, *Weapons and the Law of Armed Conflict* (Oxford University Press, 2009)

Boothby, William, 'Dehumanization: Is There a Legal Problem Under Article 36?' in Wolff Heintschel von Heinegg, Robert Frau, Tassilo Singer (eds), *Dehumanization of Warfare* (Springer, Cham, 2018) 41.

Boothby, William, 'Highly Automated and Autonomous Technologies' in William Boothby (eds), *New Technologies and the Law in War and Peace* (Cambridge University Press, 2018) 157.

Boothby, William, ‘How Far Will the Law Allow Unmanned Targeting to Go?’ in Saxon, Dan (eds), *International Humanitarian Law and the Changing Technology of War* (Martinus Nijhoff, 2013) 56

Boothby, William, *Conflict Law: The Influence of New Weapons Technology, Human Rights and Emerging Actors* (Asser, 2014) 111.

Boothby, William, *The Law of Targeting* (Oxford University Press, 2012) 89

Borenstein, Jason, ‘The Ethics of Autonomous Military Robots’ (2008) 2(1) *Studies in Ethics, Law and Technology* 13

Bothe, Michael, ‘War Crimes’ in Antonio Cassese, Paola Gaeta and John Jones (eds), *The Rome Statute of the International Criminal Court A Commentary* (OUP, 2002) 389

Bothe, Michael, Karl Josef Partsch and Waldemar A Solf, *New Rules for Victims of Armed Conflicts* (Martinus Nijhoff, 2013)

Bouchet-Saulnier, Francoise, *The Practical Guide to Humanitarian Law* (Rowman & Littlefield, 2013) 60

Boulanin, Vincent and Maaike Verbruggen, ‘Compendium on Article 36 reviews’ (2017) SIPRI Background Paper Stockholm International Peace Research Institute <https://www.sipri.org/publications/2017/sipri-background-papers/sipri-compendium-article-36-reviews>

Boulanin, Vincent, ‘Implementing Article 36 Weapon Reviews in the Light of Increasing Autonomy in Weapon Systems’ (SIPRI Insights on Peace and Security No 2015/1, Stockholm International Peace Research Institute, November 2015)

Boulanin, Vincent, ‘Mapping the Development of Autonomy in Weapon Systems: A Primer on Autonomy’ (2016) SIPRI Working Paper

Bovarnick, Jeff, Gregory Musselman et al., *Law of War Deskbook* (2011) International and Operational Law Department, The U.S. Army Judge Advocate General's Legal Center and School, Charlottesville 140.

Boylan, Patrick J, *Review of the Convention for the Protection of Cultural Property in the Event of Armed Conflict* (UNESCO, 1993) <http://unesdoc.unesco.org/images/0010/001001/100159eo.pdf>

Brownlie, Ian, *Principles of Public International Law* (Oxford University Press, 2018) 450

Bubnicki, Zdzislaw, *Modern Control Theory* (Springer, 2005)

Buchan, Russell, ‘Cyber Warfare and the Status of Anonymous under International Humanitarian Law’ (2016) 15(4) *Chinese Journal of International Law* 767

Byrnes, Michael W, ‘Nightfall: Machine Autonomy in Air-to-Air Combat’ (2014) (May-June) *Air & Space Power Journal* 48

Cahn, Naomi, ‘Poor Children: Child Witches and Child Soldiers in Sub-Saharan Africa’ (2006) 3 *Ohio State Journal of Criminal Law* 413, 418

Carey, John, William V Dunlap and R John Pritchard, *International Humanitarian Law: Origins* (Brill, 2003)

Carnahan, Burris M, ‘The Law of Land Mine Warfare: Protocol II to the United Nations Convention on Certain Conventional Weapons’ (1984) 105 *Military Law Review* 73

Carnahan, Burrus, 'Unnecessary Suffering, the Red Cross and Tactical Laser Weapons' (1996) 18 *Loyola International & Comparative Law Review* 73.

Casey, George W Jr, "America's Army in an Era of Persistent Conflict" (2008) 58 *Army* 19

Casey-Maslen, Stuart and Sharon Weill, 'The Use of Weapons in Armed Conflict' in Stuart Casey-Maslen (ed), *Weapons Under International Human Rights Law* (Cambridge University Press, 2014) 248

Cassese, Antonio 'Weapons Causing Unnecessary Suffering: Are They Prohibited?' (1975) 58 *Rivista Di Diritto Internazionale* 15

Cassese, Antonio, 'Means of Warfare: The Traditional and the New Law' in Antonio Cassese (eds), *The New Humanitarian Law of Armed* Conflict (Oceana Pubns, 1979) 161, 178

Cassese, Antonio, 'The Proper Limits of Individual Responsibility under the Doctrine of Joint Criminal Enterprise' (2007) 5 *Journal of International Criminal Justice* 109

Cassese, Antonio, 'The Statute of the International Criminal Court: Some Preliminary Reflections' (1999) 10 *European Journal of International Law* 154

Cassese, Antonio, Paola Gaeta and John R W D Jones, *The Rome Statute of the International Criminal Court: A Commentary* (Oxford University Press, 2002) vol 1

Chen, Thomas M and Saeed Abu-Nimeh, 'Lessons from Stuxnet' (2011) 44(4) *Computer* 91

Chengeta, Thompson 'Defining the Emerging Notion of 'Meaningful Human Control' in Autonomous Weapon Systems (AWS)' (2016) [Online] Available: <https://ssrn.com/abstract=2754995> [4 November 2016]

Chenwi, Lilian, *Towards the Abolition of the Death Penalty in Africa: A Human Rights Perspective* (Pretoria University Law Press, 2011) 144

Chetail, Vincent, 'The Contribution of the International Court of Justice to International Humanitarian Law' (2003) 850 *International Review of the Red Cross* 235, 253

Chinen, Mark, 'The Co-Evolution of Autonomous Machines and Legal Responsibility' (2016) 20 *Virginia Journal of Law & Technology* 338

Chopra, Samir & Laurence White, *A Legal Theory for Autonomous Artificial Agents* (University of Michigan Press, 2011) 11

Christensen, Eric, 'The Dilemma of Direct Participation in Hostilities' (2010) 19 *Journal of Transnational Law and Policy* 281

Citron Danielle, and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 *Washington Law Review* 1

Citron, Danielle Keats, 'Technological Due Process' (2008) 85 *Washington University Law Review* 1249

Clapham, Andrew & Paola Gaeta, *The Oxford Handbook of International Law in Armed Conflict* (Oxford University Press, 2014) 308

Clapham, Andrew, 'The Question of Jurisdiction Under International Criminal Law Over Legal Persons: Lessons from the Rome Conference on the International Criminal Court' in Menno Kamminga and Saman Zia-Zarifi (eds), *Liability of Multinational Corporations Under International Law* (Kluwer Law International, 2012) 195

Clark, Grant et al, 'Mind and Autonomy in Engineered Bio-systems' (1999) 12 *Engineering Applications of Artificial Intelligence* 10.

Commission on Responsibility of the Authors of the War and on Enforcement of Penalties, *Report Presented to the Preliminary Peace Conference* (29 March 1919), reprinted in (1920) 14 *American Journal of International Law* 95

Copeland, Damian P, 'Legal Review of New Technology Weapons' in Hitoshi Nasu and Robert McLaughlin (eds), *New Technologies and the Law of Armed Conflict* (Asser Press, 2014) 43

Coppin, Gilles and François Legras, 'Autonomy Spectrum and Performance Perception Issues in Swarm Supervisory Control' (2012) 100 *Proceedings of the IEEE* 592.

Cordeschi, Roberto, 'Automatic Decision-Making and Reliability in Robotic Systems: Some Implications in the Case of Robot Weapons' (2013) 28 *AI & Society* 431

Corn, Gary, 'Should the Best Offense Ever Be a Good Defense? The Public Authority to Use Force in Military Operations: Recalibrating the Use of Force Rules in the Standing Rules of Engagement' (2016) 49 *Vanderbilt Journal of Transnational Law* 48

Corn, Geoffrey, 'Autonomous Weapons Systems: Managing the Inevitability of Taking the Man Out of the Loop' in Nehal Bhuta, Susanne Beck, Robin Geiβ, Hin Liu, & Claus Kreβ (eds), *Autonomous Weapons Systems: Law, Ethics, Policy* (Cambridge University Press, 2016) 242

Coupland, Robin & Dominique Loye, 'The 1899 Hague Declaration Concerning Expanding Bullets: A Treaty Effective for More Than 100 Years Faces Complex Contemporary Issues' (2003) 849 *International Review of the Red Cross* 135, 137

Coupland, Robin, 'Humanity: What is It and How Does It Influence International Law?' (2001) 83 *International Review of the Red Cross* 969

Coupland, Robin, 'Towards a Determination of Which Weapons Cause Superfluous Injury or Unnecessary Suffering' (1997) *The SIrUS Project* ICRC 8

Crawford, Emily, *Identifying the Enemy: Civilian Participation in Armed Conflict* (Oxford University Press, 2015) 70

Crawford, James R, 'State Responsibility' in *Max Planck Encyclopedia of Public International Law* (September 2006) <http://opil.ouplaw.com/home/EPIL>

Crawford, James, *State Responsibility – The General Part* (Cambridge University Press 2013) 118

Crawford, James, *The International Law Commission's Articles on State Responsibility - Introduction, Text and Commentaries* (Cambridge University Press, 2002)

Creswell, John *Research design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th edn, Sage, 2013)

Crootof, Rebecca, 'A Meaningful Floor for "Meaningful Human Control"' (2016) *Temple International and Comparative Law Journal* 53

Crootof, Rebecca, 'The Killer Robots Are Here: Legal and Policy Implications' (2015) 36 *Cardozo Law Review* 1837

Crootof, Rebecca, 'War Torts: Accountability for Autonomous Weapons' (2016) 164 *University of Pennsylvania Law Review* 1347

Cryer, Robert et al, *An Introduction to International Criminal Law and Procedure* (Cambridge University Press, 2nd ed, 2010)

Cummings, Mary L, 'Automation and Accountability in Decision Support System Interface Design' (2006) XXXII *The Journal of Technology Studies* 23

Cummings, Mary, 'Creating Moral Buffers in Weapon Control Interface Design' (2004) *Ieee Technology and Society Magazine* 28

Cummings, Mary, 'Man Versus Machine or Man + Machine?' (2014) *Intelligent Systems*, 29(5) IEEE 62, 69

Cummings, Mary, 'Operator Interaction with Centralized Versus Decentralized UAV Architectures', in Kimon Valavanis & George Vachtsevanos (eds), *Handbook of Unmanned Aerial Vehicles* (Springer, 2015) 977

Curtin, Deirdre and André Nollkaemper, 'Conceptualizing Accountability in Public International Law' (2005) XXXVI *Netherlands Yearbook of International Law* 3

Dahl, Borge, Ditlev Tamm, *Danish Law in a European Perspective* (Forlaget Thomson, 2002)

Daoust, Isabelle, Robin Coupland and Rikke Ishoey, 'New Wars, New Weapons? The Obligation of States to Assess the Legality of Means and Methods of Warfare' (2002) 84 *International Review of the Red Cross* 345

Davis, Lynn, Michael McNerney and Michael Greenberg, 'Clarifying the Rules for Targeted Killing: An Analytical Framework for Policies Involving Long-Range Armed Drones' (2018) *RAND Corporation* 5

de Preux, Jean, 'Protocol I – Article 35 – Basic Rules' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 389

de Preux, Jean, 'Protocol I – Article 36 – New Weapons' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 421

de Preux, Jean, 'Protocol I – Article 82 – Legal Advisers in Armed Forces' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 947

Deeks, Ashley and Noam Lubell and Daragh Murray, 'Machine Learning, Artificial Intelligence, and the Use of Force by States' (2018) 10 *Journal of National Security Law and Policy* 26

den Dekker, Guido, *The Law of Arms Control: International Supervision and Enforcement* (Martinus Nijhoff, 2001)

Dinniss, Heather & Jann Kleffner, 'Soldier 2.0: Military Human Enhancement and International Law' (2016) 92 *International Law Studies US Naval War College* the Stockton Center for the Study of International Law 434

Dinniss, Heather, *Cyber Warfare and the Laws of War* (Cambridge University Press, 2012) 65

Dinstein, Yoram, *Non-International Armed Conflicts in International Law* (Cambridge University Press, 2014) 180

Dinstein, Yoram, *The Conduct of Hostilities under the Law of International Armed Conflict* (Cambridge University Press, 2nd ed, 2010)

Diskant, Edward, 'Comparative Corporate Criminal Liability' (2008) 118 *Yale Law Journal* 140

Doria, Jose et al, *The Legal Regime of the International Criminal Court: Essays in Honour of Professor Igor Blishchenko [1930-2000]* (Brill, 2009) 144

Dörmann, Knut, 'Preparatory Commission for the International Criminal Court: The Elements of War Crimes' (2000) 82 *International Review of the Red Cross* 771

Dormann, Knut, 'The Legal Situation of Unlawful/Unprivileged Combatants' (2003) 85(849) *Revue Internationale De La Croix-Rouge/International Review of the Red Cross* 46

Dörmann, Knut, *Elements of War Crimes under the Rome Statute of the International Criminal Court* (Cambridge University Press, 2003)

Doswald-Beck, Louise, *San Remo Manual on International Law Applicable to Armed Conflicts at Sea* (Cambridge University Press, 1995)

Drumbl, Mark A, 'Accountability for System Criminality' (2010) 8 *Santa Clara Journal of International Law* 373

Duff, Anthony, *Intention, Agency, and Criminal Liability* (Blackwell, 1990) 162

Duffy, Helen, *The War on Terror and the Framework of International Law* (Cambridge University Press, 2015) 369

Dunant, Henry, *A Memory of Solferino* (ICRC, 2006)

Dunlap, Charles J, 'Accountability and Autonomous Weapons: Much Ado about Nothing?' (2016) 30 *Temple International and Comparative Law Journal* 63

Dunning, David, Judith Meyerowitz and Amy Holzberg, 'Ambiguity in Self-Evaluation: The Role of Idiosyncratic Trait Definitions in Self-Serving Assessments of Ability' (1989) 57 (6) *Journal of Personality and Social Psychology* 1082

Dupuy, Pierre, 'Reviewing the Difficulties of Codification: on Ago's Classification of Obligations of Means and Obligations of Result in Relation to State Responsibility' (1999) 10 *European Journal of International Law* 371

Dupuy, Pierre, *Due Diligence in the International Law of State Responsibility*, OECD: Legal Aspects of Trans frontier Pollution (OECD, 1977)

Durham, Helen and Eve Massingham, 'Moving from the Mechanics of Accountability to a Culture of Accountability: What More Can be Done in Addition to Prosecuting War Crimes?' in Jadranka Petrovic (ed), *Accountability for Violations of International Humanitarian Law: Essays in Honour of Tim McCormack* (Routledge, 2016) 267

Dworkin, Gerald, *The Theory and Practice of Autonomy* (Cambridge University Press, 1988) 6

Ebbesson, Jonas et al, *International Law and Changing Perceptions of Security: Liber Amicorum Said Mahmoudi* (Brill, 2014)

Efrony, Dan & Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' (2018) 112(4) *American Journal of International Law* 657

Egeland, Kjolv, 'Lethal Autonomous Weapon Systems under International Humanitarian Law' (2016) 85 *Nordic Journal of International Law*

Eichensehr, Kristen, 'On Target? The Israeli Supreme Court and the Expansion of Targeted Killings' (2007) 116 *Yale Law Journal* 1873

Ekberg, Peter J, 'Remotely Delivered Landmines and International Law' (1995) 33 *Columbia Journal of Transnational Law* 149

Ekelhof, Merel, 'Lifting the Fog of Targeting: Autonomous Weapons and Human Control Through the Lens of Military Targeting' (2018) 71 *Naval War College Review* 68

Elliot, Catherina, 'The French Law of Intent and its Influence on the Development of International Criminal Law' (2010) 11 *Criminal Law Forum* 35, 46

Elliott, Lisa & Bryan Stewart, 'Automation and Autonomy in Unmanned Aircraft Systems' in Richard Barnhart et al. (eds), *Introduction to Unmanned Aircraft Systems* (Taylor & Francis, 2011) 290

Eser, Albin, 'Mental Elements–Mistake of Fact and Mistake of Law' in Antonio Cassese, Paola Gaeta and John Jones (eds), *The Rome Statute of the International Criminal Court A Commentary* (OUP, 2002) 899

Etzioni, Amitia and Etzioni Oren, 'Pros and Cons of Autonomous Weapons Systems' (2017) *Military Review* 1

Eyffinger, Arthur, *The 1899 Hague Peace Conference: The Parliament of Man, the Federation of the World* (Martinus Nijhoff, 1999)

Fenrick, William J, 'The Rule of Proportionality and Protocol I in Conventional Warfare' (1982) 98 *Military Law Review* 91

Fenrick, William, 'A First Attempt to Adjudicate Conduct of Hostilities Offences: Comments on Aspects of the ICTY Trial Decision in the Prosecutor v. Tihomir Blaskic' (2000) 13 *Leiden Journal of International Law* 931, 940

Ferzan, Kimberly, 'Opaque Recklessness' (2001) 91 *Journal of Criminal Law and Criminology* 597, 599

Ferzan, Kimberly, Larry Alexander and Stephen Morse, *Crime and Culpability: A Theory of Criminal Law* (Cambridge University Press, 2009) 71

Final Record of the Diplomatic Conference Convened by the Swiss Federal Council for the Establishment of International Conventions for the Protection of War Victims and Held at Geneva from April 21st to August 12th, 1949 (Federal Political Department, Berne) vol IIB Finn, Anthony and Steve Scheding, Developments and Challenges for Autonomous Unmanned Vehicles (Springer, 2010)

Finkelstein, Claire et al, *Targeted Killings: Law and Morality in an Asymmetrical World* (Oxford University Press, 2012) 68

Finnin, Sarah, 'Mental Elements under Article 30 of the Rome Statute of the International Criminal Court: A Comparative Analysis' (2012) 61 *International and Comparative Law Quarterly* 355

Fischel, Daniel and Alan Sykes, 'Corporate Crime' (1996) 25 *Journal of Legal Studies* 319

Fisher, Michael et al., 'Verifying Autonomous Systems: Exploring Autonomous Systems and the Agents That Control Them' (2013) 56 *Communications of the ACM* 84

Fleck, Dieter, 'Individual and State Responsibility for Violations of the Ius in Bello: An Imperfect Balance' in Wolff Heintschel von Heinegg and Volker Epping (eds), *International Humanitarian Law Facing New Challenges* (Springer, 2007)

Fleck, Dieter, *The Handbook of International Humanitarian Law* (Oxford University Press, 2013) 13

Fleischman, William, 'Just Say No! to Lethal Autonomous Robotic Weapons' (2015) 13 *Journal of Information, Communication and Ethics in Society* 313

Ford, Christopher, 'Autonomous Weapons and International Law' (2017) 69 *The South Carolina Law Review* 413

Francioni, Francesco & Natalino Ronzitti, *War by Contract: Human Rights, Humanitarian Law, and Private Contractors* (Oxford University Press, 2011) 213

Francioni, Francesco, 'Private Military Contractors and International Law: An Introduction' (2008) 19 *European Journal of International Law* 961

François, Charles (eds), *International Encyclopedia of Systems and Cybernetics* (K G Saur, 2nd ed, 2004) vol 1

Fry, James, 'Contextualized Legal Reviews for the Means and Methods of Warfare: Cave Combat and International Humanitarian Law' (2006) 44 *Columbia Journal of Transnational Law* 453

Fulford, Adrian, 'Foreword' (2003) in Ilias Bantekas & Susan Nash (eds), *International Criminal Law* (Routledge, 2003)

Fussell, Susan R et al, 'How People Anthropomorphize Robots' (2008) *Proceedings of the 3rd ACM/IEEE International Conference on Human Robot Interaction* 145

Fuzaylova, Elizabeth, 'War Torts, Autonomous Weapon Systems, and Liability: Why a Limited Strict Liability Tort Regime Should Be Implemented' (2019) 40 *Cardozo Law Review* 1356

Gaeta, Paola, 'Autonomous Weapon Systems and the Alleged Responsibility Gap' Speaker's Summary in *Expert Meeting, Autonomous Weapon Systems Implications of Increasing Autonomy in the Critical Functions of Weapons (Versoix, Switzerland, 15–16 March 2016)*, ed. ICRC, Geneva: ICRC 45

Galliott, Jai and Tim McFarland, 'Autonomous Systems in a Military Context (Part 2): A Survey of the Legal Issues' (2016) *International Journal of Robotics Applications and Technologies* 62

Galliott, Jai and Tim McFarland, 'Autonomous Systems in a Military Context (Part 1): A Survey of the Legal Issues' (2016) *International Journal of Robotics Applications and Technologies* 42

Galliott, Jai, *Military Robots: Mapping the Moral Landscape* (Routledge, 2015) 270

Garraway, Charles, 'The Application of Superior Responsibility in An Era of Unlimited Information' in Dan Saxon (eds), *International Humanitarian Law and the Changing Technology of War* (Martinus Nijhoff, 2013) 203

Gasser, Hans-Peter, 'A Look at the Declaration of St. Petersburg of 1868' (1993) 33 *International Review of the Red Cross* 511

Geiss, Robin, 'The International-Law Dimension of Autonomous Weapons Systems' (Study, Friedrich-Ebert-Stiftung, International Policy Analysis, October 2015)

Geiss, Robin, and Henning Lahmann, ‘Autonomous Weapons Systems: A Paradigm Shift for the Law of Armed Conflict’ in Jens David Ohlin (eds), *Research Handbook on Remote Warfare* (Edward Elgar, 2016) 392

Geneva Academy of International Humanitarian Law ‘Autonomous Weapon Systems under International Law’ (2014) *Academy Briefing Number 8* 24

Gill, Terry, Jelle Van Haaster & Mark Roorda, ‘Some Legal and Operational Considerations Regarding Remote Warfare’ in Jens David Ohlin (eds), *Research Handbook on Remote Warfare* (Eldward Elgar Publishers, 2017) 298

Gillard, Emanuela, ‘Proportionality in the Conduct of Hostilities The Incidental Harm Side of the Assessment Proportionality in the Conduct of Hostilities’ Chatham House Report, 2018 6

Gillespie, Tony and Robin West, ‘Requirements for Autonomous Unmanned Air Systems set by Legal Issues’ (2010) 4(2) *The International C2 Journal* 1

Gilliland, Jane, ‘Submarines and Targets: Suggestions for New Codified Rules of Submarine Warfare’ (1985) 73 *The Georgetown Law Journal* 975, 1002

Ginsberg, Matt, *Essentials of Artificial Intelligence* (Newnes, 2012)

Goodman, Ryan and Derek Jinks, ‘The ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law: An Introduction to the Forum’ (2010) 42 *New York University Journal of International Law and Politics* 640

Goodrich, Michael A and Alan C Schultz, ‘Human-Robot Interaction: A Survey’ (2007) 1 *Foundations and Trends in Human-Computer Interaction* 203

Goppel, Anna, *Killing Terrorists: A Moral and Legal Analysis* (De Gruyter, 2013) 308

Greenwood, Christopher, 'Battlefield Laser Weapons in the Context of the Law on Conventional Weapons' in Louise Doswald-Beck (eds), *Blinding Weapons, Reports of the Meetings of Experts Convened by the International Committee of the Red Cross on Battlefield Laser Weapons* 1989-1991 (International Committee of the Red Cross, 1993) 71

Greenwood, Christopher, 'Customary Law Status of the 1977 Geneva Protocols' in Astrid J M Delissen and Gerard J Tanja (eds), *Humanitarian Law of Armed Conflict: Challenges Ahead: Essays in Honour of Frits Kalshoven* (Martinus Nijhoff, 1991) 111

Grimmelmann, James, 'Regulation by Software' (2005) 114 *Yale Law Journal* 1719

Gross, Oren, When Machines Kill: Criminal Responsibility for International Crimes Committed by Lethal Autonomous Robots, Address at the We Robot 2012 Conference: Military Robotics Panel Presentation (22 April 2012)

Grover, Leena, 'A Call to Arms: Fundamental Dilemmas Confronting the Interpretation of Crimes in the Rome Statute of the International Criminal Court' (2010) *European Journal of International Law* 543

Grover, Sonja, *The Torture of Children During Armed Conflicts: The ICC's Failure to Prosecute and the Negation of Children's Human Dignity* (Springer, 2013) 93

Grut, Chantal, 'The Challenge of Autonomous Lethal Robotics to International Humanitarian Law' (2013) 18(1) *Journal of Conflict & Security Law* 5

Guarini, Marcello & Paul Bello, 'Robotic Warfare: Some Challenges in Moving from Non-Civilian to Civilian Theaters' in Patrick Lin and others (eds), *Robot Ethics: The Ethical and Social Implications of Robotics* (MIT Press, 2012) 149, 150

Hall, Christopher Keith, 'The First Proposal for an International Criminal Court' (1998) 38 *International Review of the Red Cross* 57

Hammond, Daniel N, 'Autonomous Weapons and the Problem of State Accountability' (2015) 15 *Chicago Journal of International Law* 652

Hancock, Peter A and Stephen F Scallen, 'Allocating Functions in Human–Machine Systems' in Robert R Hoffman, Michael F Sherrick and Joel S Warm (eds), *Viewing Psychology as a Whole: The Integrative Science of William N Dember* (American Psychological Association, 1998) 521

Hangos, Katalin M, Rozália Lakner and Miklós Gerzson, *Intelligent Control Systems: An Introduction with Examples* (Kluwer Academic Publishers, 2004)

Hart, Herbert, *Punishment and Responsibility: Essays in the Philosophy of Law* (Oxford University Press, 2008) 227

Hassing, Richard, *Final Causality in Nature and Human Affairs* (The Catholic University of America Press, 1997) 37

Hayashi, Nobuo, 'Military Necessity as Normative Indifference' (2013) 44 *Georgetown Journal of International Law* 675

Hazen, H L, 'Theory of Servo-Mechanisms' (1934) 218(3) *Journal of the Franklin Institute* 279

Hearst, Marti A, 'Trends & Controversies: Mixed-Initiative Interaction' (1999) 14(5) *IEEE Intelligent Systems* 14

Henckaerts, Jean-Marie and Louise Doswald-Beck, *Customary International Humanitarian Law* (Cambridge University Press, 2005) vols 1 and 2

Henderson, Ian, Patrick Keane and Josh Liddy, 'Remote and Autonomous Warfare Systems: Precautions in Attack and Individual Accountability' in Jens David Ohlin (eds), *Research Handbook on Remote Warfare* (Edward Elgar, 2016) 358

Henderson, Ian, *The Contemporary Law of Targeting* (Martinus Nijhoff, 2009)

Henderson, Ian, *The Contemporary Law of Targeting: Military Objectives, Proportionality and Precautions in Attack under Additional Protocol I* (Martinus Nijhoff Publishers, 2009) 36.

Hennessy, Michael A and B J C McKercher (eds), *War in the Twentieth Century: Reflections at Century's End* (Praeger, 2003)

Hensel, Howard, *The Law of Armed Conflict: Constraints on the Contemporary Use of Military Force* (Routledge, 2007) 172

Herbach, Jonathan David, 'Into the Caves of Steel: Precaution, Cognition and Robotic Weapon Systems Under the International Law of Armed Conflict' (2012) 4(3) *Amsterdam Law Forum* 3

Herring, Jonathan, *Criminal Law: Text, Cases, and Materials* (Oxford University Press, 2018) 391

Hessbruegge, Jan, 'The Historical Development of the Doctrines of Attribution and Due Diligence in International Law' (2004) 36 *New York University Journal of International Law and Politics* 265

Heyns, Christof & Sarah Knuckey, 'The Long-term International Law Implications of Targeted Killing Practices' (2013) 54 *Harvard International Law Journal* 114

Heyns, Christof, 'Autonomous Weapons Systems: Living a Dignified Life and Dying a Dignified Death' in Nehal Bhuta et al. (eds), *Autonomous Weapons Systems: Law, Ethics, Policy* (Cambridge University Press, 2016) 20

Heyns, Christof, 'Human Rights and the Use of Autonomous Weapons Systems (AWS) During Domestic Law Enforcement' (2016) 38 *Human Rights Quarterly* 350

Heyns, Christof, Dapo Akande, Lawrence Hill-Cawthorne and Thompson Chengeta, 'The International Law Framework Regulating the Use of Armed Drones' (2016) 65 (4) *International and Comparative Law Quarterly* 791

Hollis, Duncan, 'Setting the Stage: Autonomous Legal Reasoning in International Humanitarian Law' (2016) 5 *Temple International and Comparative Law Journal* 4.

Homayounnejad, Maziar, 'Assessing the Sense and Scope of Autonomy in Emerging Military Weapon Systems' (August 24, 2017). TLI Think! Paper 76/2017. Available at SSRN: https://ssrn.com/abstract=3027540 or http://dx.doi.org/10.2139/ssrn.3027540 15.

Hoppe, Carsten, 'Passing the Buck: State Responsibility for Private Military Companies' (2008) 19 *European Journal of International Law* 989

Horder, Jeremy, *Ashworth's Principles of Criminal Law* (Oxford University Press, 2009) 10

Horowitz, Michael C and Paul Scharre, 'Meaningful Human Control in Weapon Systems: A Primer' (Working Paper, Center for a New American Security, March 2015)

HPRC, *Manual on International Law Applicable to Air and Missile Warfare* (2009)

Hughes, Joshua, 'The Law of Armed Conflict Issues Created by Programming Automatic Target Recognition Systems Using Deep Learning Methods' in Terry Gill, Robin Geiss, Heike Krieger, Christophe Paulussen (eds) *Yearbook of International Humanitarian Law* (The Hague: T.M.C. Asser Press, 2019) 123

Human Rights Watch, 'Killer Robots and the Concept of Meaningful Human Control' (Memorandum to CCW Delegates, April 2016) 10 < https://www.hrw.org/sites/default/files/supporting_resources/robots_meaningful_human _control_final.pdf>

Human Rights Watch, *Losing Humanity: The Case Against Killer Robots* (November 2012)

Human Rights Watch, *Mind the Gap: The Lack of Accountability for Killer Robots* (April 2015)

Human Rights Watch, *Off Target: The Conduct of the War and Civilian Casualties in Iraq* (2003) Summary and Recommendations <https://www.hrw.org/reports/2003/usa1203/usa1203_sumrecs.pdf>

Human Rights Watch, *Shaking the Foundations: The Human Rights Implications of Killer Robots* (2014)

Hunter, Dan, 'Reason is Too Large: Analogy and Precedent in Law' (2001) 50 *Emory Law Journal* 1197

Husak, Douglas, 'Negligence, Belief, Blame and Criminal Liability: The Special Case of Forgetting' (2011) 5 *Criminal Law and Philosophy* 202

Ian Lloyd, *Information Technology Law* (Oxford University Press, 2011)

International Committee of the Red Cross, 'A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977' (2006) 88 *International Review of the Red Cross* 931

International Committee of the Red Cross, 'Autonomous Weapon Systems: Implications Of Increasing Autonomy In The Critical Functions Of Weapons' (Report on Expert Meeting, Versoix, Switzerland, 15-16 March 2016)

International Committee of the Red Cross, *Conference of Government Experts on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts, 24 May -12 June, 1971 (1971)* vol III: Protection of the Civilian Population Against Dangers of Hostilities

International Committee of the Red Cross, *Conference of Government Experts on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts, Second Session, 3 May -3 June 1972 – Report on the Work of the Conference* (1972) vol I

International Committee of the Red Cross, *Conference of Government Experts on the Use of Certain Conventional Weapons (Lucerne, 24.9-18.10.1974): Report* (1975)

International Committee of the Red Cross, *Conference of Government Experts on the Use of Certain Conventional Weapons (Second Session - Lugano, 28.1-26.2.1976): Report* (1976)

International Committee of the Red Cross, *Draft Additional Protocols to the Geneva Conventions of August 12, 1949 – Commentary* (1973)

International Society of Military Law and the Laws of War, *Armed Forces and the Development of the Law of War (Ninth International Congress, Lausanne, 2–6 September 1982)* (1982)

Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law: Adopted by the Assembly of the International Committee of the Red Cross on 26 February 2009 *International Review of the Red Cross*, 90(872), 991-1047

Jacobsson, Marie, 'Modern Weaponry and Warfare: The Application of Article 36 of Additional Protocol I by Governments' in Anthony Helm (eds), *The Law of War in the 21st Century: Weaponry and the Use of Force International Law Studies* (Naval War College Press, 2007) 184

Jain, Neha, 'The Control Theory of Perpetration in International Criminal Law' (2011) 12 *Chicago Journal of International Law* 172

Jakobsh, Doris, *Sikhism* (University of Hawaii Press, 2012) 60

Jenks, Chris, 'False Rubicons, Moral Panic, & Conceptual Cul-De-Sacs: Critiquing & Reframing the Call to Ban Lethal Autonomous Weapons' (2016) 44(1) *Pepperdine Law Review* (Article 2)

Jensen, Eric, 'Direct Participation in Hostilities' in William Banks (eds), *New Battlefields Old Laws: Critical Debates on Asymmetric Warfare* (Columbia University Press, 2011)

Jensen, Eric, 'The Tallinn Manual 2.0: Highlights and Insights' (2017) 48 *Georgetown Journal of International Law* 735

Jensen, Erik 'The Future of the Law of Armed Conflict: Ostriches, Butterflies, and Nanobots' (2014) 35 *Michigan Journal of International Law* 253

Jescheck, Hans, 'The General Principles of International Criminal Law Set Out in Nuremberg, as Mirrored in the ICC Statute' (2004) 2 *Journal of International Criminal Justice* 38,45

Jevglevskaja, Natalia, 'Legal Review of New Weapons: Origins of Article 36 AP I' (2018) 25 *The Finnish Yearbook of International Law* 320

Jevglevskaja, Natalia, 'Weapons Review Obligation under Customary International Law' (2018) 94 *International Law Studies* 185, 221

Jha, UC, *Killer Robots: Lethal Autonomous Weapon Systems Legal, Ethical and Moral Challenges* (VIJ Books, 2017)

Jiho, Hanrei, '*Shimoda v State of Japan'* (1964) 8 *Japanese Annual of International Law* 242

Jinks, Derek et al, *Applying International Humanitarian Law in Judicial and Quasi-Judicial Bodies: International and Domestic Aspect* (Asser Press, 2014) 79

Johannson, Linda, 'Is it Morally Right to Use Unmanned Aerial Vehicles (UAVs) in War?' (2011) 24 *Philosophy and Technology* 279, 291

Johnson, Aaron, 'The Morality of Autonomous Robots' (2013) 12 *Journal of Military Ethics* 134

Johnson, Deborah G, 'Software Agents, Anticipatory Ethics, and Accountability' in Gary E Marchant, Braden R Allenby and Joseph R Herkert (eds), *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem* (Springer, 2011) 61

Jones, John & Steven Powles, *International Criminal Practice* (Oxford University Press, 2003) 415

Jones, Troy & Leammukda, Mitch, 'Requirements-Driven Autonomous System Test Design: Building Trust Relationships (2010) 1 International Test and Evaluation Association (ITEA) Live Virtual Constructive Conference, El Paso, TX, January 11-14

Joshi, Shashank, & Stein Aaron, 'Emerging Drone Nations' Survival' (2013) 55 *Global Politics and Strategy* 53, 78

Kaeb, Caroline, 'The Shifting Sands of Corporate Liability Under International Criminal Law' (2016) 49 *The George Washington International Law Review* 385

Kaku, Michio, *The Future of the Mind: The Scientific Quest to Understand, Enhance, and Empower the Mind* (Overseas Editions New 2014) 17

Kalshoven, Frits, 'State Responsibility for Warlike Acts of the Armed Forces' (1991) 40 *International and Comparative Law Quarterly* 827

Kanwar, Vik 'Post-Human Humanitarian Law: The Law of War in the Age of Robotic Warfare' (2011) 2 *Harvard Journal of National Security* 3

Karnow, Curtis E A, 'The Application of Traditional Tort Theory to Embodied Machine Intelligence' in Calo, Ryan, A Michael Froomkin and Ian Kerr (eds), *Robot Law* (Edward Elgar, 2016) 54

Kastan, Benjamin, 'Autonomous Weapons Systems: A Coming Legal "Singularity"?' (2013) *Journal of Law, Technology & Policy* 45

Keeley, Tom, 'Auditable Policies for Autonomous Systems' Paul Sharre & Andrew Williams (eds), *Autonomous Systems: Issues for Defence Policymakers* (Nato, 2015) 221

Keith, Kirsten, 'The Mens Rea of Superior Responsibility as Developed by ICTY Jurisprudence' (2001) 14(3) *Leiden Journal of International Law* 617, 634

Kessler, Birgit, 'The Duty to Ensure Respect under Common Article 1 of the Geneva Conventions' (2001) *German Yearbook of International Law* 498

Khanna, Vikramaditya, 'Corporate Criminal Liability, What Purpose Does It Serve?' (1996) 109 *Harvard Law Review* 1489

Kindall, MPA, 'Immunity of States for Non-commercial Torts: A Comparative Anaysis of the International Law Commission's Draft' (1987) 75 *California Law Review* 1849

King, Matt, 'The Problem with Negligence' (2009) 35 *Social Theory and Practice* 577, 594

Kiss, Alex and Dinah Shelton, 'Strict Liability in International Environmental Law' in Tafsir Malick Ndiaye and Rüdiger Wolfum (eds), *Law of the Sea, Environmental Law and Settlement of Disputes: Liber Amicorum Judge Thomas A. Mensah* (Brill, 2007) 1148

Klamberg, Mark, 'Exploiting Legal Thresholds, Fault-Lines and Gaps in the Context of Remote Warfare' in Jens David Ohlin (eds), *Research Handbook on Remote Warfare* (Edward Elgar, 2016) 203

Kleffner, Jann K, 'From 'Belligerents' to 'Fighters' and Civilians Directly Participating in Hostilities – On the Principle of Distinction in Non-International Armed Conflicts One Hundred

Years After the Second Hague Peace Conference' (2007) 54 *Netherlands International Law Review* 315

Kleffner, Jann, 'Sources of the Law of Armed Conflict' in Rain Liivoja and Tim McCormack (eds), *Routledge Handbook of the Law of Armed Conflict* (Routledge, 2016) ch 4

Klip, Andre & Steven Freeland, *Annotated Leading Cases of International Criminal Tribunals: The International Criminal Tribunal for the Former Yugoslavia* (Intersentia, 2001) 321

Knuchel, Sevrine, 'State Immunit and the Promise of Jus Cogens' (2011) 9 *Northwestern University Journal of International Human Rights* 154

Kreps, Sarah, 'Flying Under the Radar: A Study of Public Attitudes Towards Unmanned Aerial Vehicles' (2014) 1(1) *Research & Politics*

Krishnan, Armin, *Killer Robots: Legality and Ethicality of Autonomous Weapons* (Ashgate, 2009)

Krupiy, Tetyana, 'Of Souls, Spirits and Ghosts: Transposing the Application of the Rules of Targeting to Lethal Autonomous Robots' (2016) 16(1) *Melbourne Journal of International Law* 145

Krupiy, Tetyana, 'Unravelling Organisational Power Dynamics: Towards a Theory of Accountability for Crimes Triggered by Lethal Autonomous Weapon Systems' (2017) 15 *Loyola University Chicago International Law Review* 19

Kumagai, Jean, 'A Robotic Sentry for Korea's Demilitarized Zone' (2007) 44 *Institute of Electrical and Electronics Engineers Spectrum* 2

Kuptel, Artur and Andy Williams, Policy Guidance: Autonomy in Defence Systems (29 October 2014). Available at SSRN: <https://ssrn.com/abstract=2524515>

Landau, I D, R Lozano and M M'Saad, *Adaptive Control* (Springer, 1998)

Larionov, Victor, 'Russian Military Doctrine/Strategy, Future Security Threats and Warfare' in Sharyl Cross et al. (eds), *Global Security Beyond the Millennium: American and Russian Perspectives* (Palgrave Macmillan, 1999) 238

Lawand, Kathleen, 'Reviewing the Legality of New Weapons, Mean and Methods of Warfare' (2006) 88 *International Review of the Red Cross* 926

Lazarski, Anthony, 'Legal Implications of the Uninhabited Combat Aerial Vehicle' (2002) 16 *Aerospace Power Journal* 74

Leigh, James R, *Control Theory: A Guided Tour* (Institution of Engineering and Technology, 2012)

Lennon, Genevieve, *Routledge Handbook of Law and Terrorism* (Routledge, 2015) 58

Leveringhaus, Alex, *Ethics and Autonomous Weapons* (Palgrave Macmillan, 2016) 114

Levie, Howard, *Protection of War Victims: Protocol I to the 1949 Geneva Conventions* (Oceana Publications, 1980) 287

Lewis, Dustin, Gabriella Blum, and Naz Modirzadeh, War-Algorithm Accountability 62, (Harvard Law School Program on International Law and Armed Conflict, 2016), available at http://pilac.law.harvard.edu/waa/ 16.

Lewis, John 'The Case for Regulating Fully Autonomous Weapons' (2015) 124 *Yale Law* Journal 1309

Lieber, Francis, *Instructions for the Government of Armies of the United States in the Field* (Government Printing Office, 1898) [originally issued as: General Orders No 100, Adjutant General's Office, 1863]

Lieblich, Eliav and Eyal Benvenisti, 'The Obligation to Exercise Discretion in Warfare: Why Autonomous Weapons Systems are Unlawful' in Nehal Bhuta et al (eds), *Autonomous Weapons Systems: Law, Ethics, Policy* (Cambridge University Press, 2016) 245

Liivoja, Rain, Kobi Leins and Tim McCormack, 'Emerging Technologies of Warfare' in Rain Liivoja and Tim McCormack (eds), *Routledge Handbook of the Law of Armed Conflict* (Routledge, 2016) ch 35

Lin, Patrick et al, *Robot Ethics: The Ethical and Social Implications of Robotics* (MIT Press, 2014)

Lin, Patrick, 'Introduction to Robot Ethics' in Patrick Lin and others (eds), *Robot Ethics: The Ethical and Social Implications of Robotics* (MIT Press, 2012) 8

Lin, Patrick, George Bekey, and Keith Abney, 'Autonomous Military Robotics: Risk, Ethics, and Design' (2008) California Polytechnic State University San Luis Obispo 78

Linkens, D A and H O Nyongesa, 'Learning Systems in Intelligent Control: An Appraisal of Fuzzy, Neural and Genetic Algorithm Control Applications' (2002) 143(4) *IEE Proceedings - Control Theory and Applications* 367

Liu, Hin, 'Refining Responsibility: Differentiating Two Types of Responsibility Issues Raised by Autonomous Weapons Systems' (2016) in Nehal Bhuta, Susanne Beck, Robin Geiβ, Hin Liu, & Claus Kreβ (eds), *Autonomous Weapons Systems: Law, Ethics, Policy* (Cambridge University Press, 2016) 337

Liu, Hin-Yan, 'Categorization and Legality of Autonomous and Remote Weapons Systems' (2012) 94 *International Review of the Red Cross* 627

Luna, Erik, 'The Curious Case of Corporate Criminality' (2009) 46 *American Criminal Law Review* 1507

Lytton, Christopher, 'Blood for Hire: How the War in Iraq Has Reinvented the World's Second Oldest Profession' (2006) 8 *Oregon Review of International Law* 307

Malik, Swati, 'Autonomous Weapon Systems: The Possibility and Probability of Accountability' (2018) 35 *Wisconsin International Law Journal* 634

Mantei, Marilyn, 'The Effect of Programming Team Structures on Programming Tasks' (2011) 24 *Communications of the ACM* 106

Maogoto, Jackson, *Technology and the Law on the Use of Force* (Routledge, 2015)

Marchant, Gary E et al, 'International Governance of Autonomous Military Robots' (2011) XII *Columbia Science and Technology Law Review* 272

Marchuk, Iryna, *The Fundamental Concept of Crime in International Criminal Law: A Comparative Law Analysis* (Springer, 2013) 134

Margulies, Peter, 'The Other Side of Autonomous Weapons: Using Artificial Intelligence to Enhance IHL Compliance' in Ronald Alcala and Eric Talbot Jensen (eds), *The Impact of Emerging Technologies on the Law of Armed Conflict* (Oxford University Press, 2018) 156

Margulies, Peter, 'Making Autonomous Weapons Accountable: Command Responsibility for Computer-Guided Lethal Force in Armed Conflicts' in Jens David Ohlin (eds), *Research Handbook on Remote Warfare* (Edward Elgar, 2016) 442

Marra, William and McNeil, Sonia, 'Understanding "the loop": Regulating the Next Generation of War Machines' (2013) 36 *Harvard Journal of Law and Public Policy* 1155

Maslen, Stuart, 'Autonomous Weapons Systems and International Criminal Law' in Stuart Maslen, Nathalie Weizmann, Maziar Homayounnejad, & Hilary Stauffer (eds), *Drones and Other Unmanned Weapons Systems under International Law* (Brill, 2018) 245

Matheson, Michael, 'The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions' (1987) 2 *Amsterdam University Journal of International Law and Policy* 419, 420

Matthee Marielle et al, *Armed Conflict and International Law: In Search of the Human Face: Liber Amicorum in Memory of Avril McDonald* (Asser Press, 2013)

Matthias, Andreas, 'The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata (2014) 6 *Ethics and Information Technology* 176

Matthisas, Andreas, *Automata as Holders of Rights. A Proposal for a Change in Legislation* (Logos Verlag, 2010) 37

Maurer, Peter, 'War, Protection and the Law' FCO International Law Lecture, 19 May 2014, London. Available online at <https://www.icrc.org/eng/resources/documents/statement/05-23-war-protection-and-the-law-icrc-approach-fco-2nd-international-law-lecture-19-may-2014.htm>

Mazzeschi, Riccardo, 'The Due Diligence Rule and the Nature of the International Responsibility of States' (1992) 35 *German Yearbook of International Law* 47

McClelland, Justin, 'The Review of Weapons in Accordance with Article 36 of Additional Protocol I' (2003) 85 *International Review of the Red Cross* 397

McCormack, Timothy & Avril McDonald, *Yearbook of International Humanitarian Law* (T.M.C. Asser Press 2006) 84

McCormack, Timothy L H, 'Their Atrocities and Our Misdemeanours: The Reticence of States to Try Their 'Own Nationals' for International Crimes' in Mark Lattimer and Philippe Sands (eds), *Justice for Crimes Against Humanity* (Hart Publishing, 2003) 107.

McDonald, Avril, 'The International Legality of Depleted Uranium Weapons' Presentation at the Symposium on the Health Impact of Depleted Uranium Munitions' 26-27 (June 14, 2003), http://www.nuclearpolicy.org/files/nuclear/mcdonald-jun-14 03.pdf

McDonald, Henry, 'Ex-Google Worker Fears Killer Robots' Could Cause Mass Atrocities' *The Guardian* (London, 15 September 2019)

McDougal, Myres & Florentino Feliciano, *Law and Minimum World Public Order* (Yale University Press, 1961) 616.

McFarland, Tim and Tim McCormack, 'Mind the Gap: Can Developers of Autonomous Weapons Systems be Liable for War Crimes?' (2014) 90 *International Law Studies* 361

McLaughlin, Rob, 'Unmanned Naval Vehicles at Sea: USVs, UUVs, and the Adequacy of the Law' (2011) 21(2) *Journal of Law, Information and Science* 100

McNeal, Gregory, 'Targeted Killing and Accountability' (2014) 102 *Georgetown Law Journal* 681, 685

Meeran, Richard, 'Tort Litigation Against Multinational Corporations for Violations of Human Rights' (2011) 3 *City University of Hong Kong Law Review* 5

Meier, Michael W, 'Lethal Autonomous Weapons Systems (LAWS): Conducting a Comprehensive Weapons Review' (2016) 30 *Temple International and Comparative Law Journal* 119

Meier, Michael, 'Lethal Autonomous Weapons Systems - Is It the End of the World as We Know It... Or Will We Be Just Fine' in Winston Williams and Christopher Ford (eds), *Complex Battlespaces the Law of Armed Conflict and the Dynamics of Modern Warfare* (Oxford University Press, 2019) 328

Meloni, Chantal, *Command Responsibility in International Criminal Law* (T.M.C. Asser Press, 2010) 3

Melzer, Nils, '*Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law'* (ICRC, 2009) available online <https://www.icrc.org/eng/assets/files/other/irrc-872reports-documents.pdf> accessed on 5 August 2018 at 65

Melzer, Nils, *Human Rights Implications of the Usage of Drones and Unmanned Robots in Warfare*, Study, European Parliament, Directorate-General for External Policies, Policy Department, May 2013, 19

Mettraux, Guenael, *The Law of Command Responsibility* (Oxford University Press, 2009) 156

Moore, Michael and Heidi Hurd, 'Punishing The Awkward, The Stupid, The Weak, and The Selfish: The Culpability of Negligence' (2011) 5 *Criminal Law and Philosophy* 150

Mostajelean, Bahareh, 'Foreign Alternatives to the Alien Tort Claims Act: The Success or Is It Failure? of Bringing Civil Suits Against Multinational Corporations That Commit Human Rights Violations' (2008) 40 *The George Washington International Law Review* 497

Mull, Nicholas, 'The Roboticization of Warfare with Lethal Autonomous Weapon Systems (Laws): Mandate of Humanity or Threat to It?' (2017) *Houston Journal of International Law* 63

Muller, Vincent, ‘Autonomous Killer Robots are Probably Good News’ (2016) in Ezio Di Nucci & Fllippo Santonio de Sio (eds), *Drones and Responsibility: Legal, Philosophical and Socio-technical Perspectives on the Use of Remotely Controlled Weapons* (Routledge, 2016) 67, 81

Myers, Glenford J, *The Art of Software Testing* (John Wiley & Sons, 2nd ed, 2004)

NIST Engineering Laboratory, ‘Autonomy Levels for Unmanned Systems’ (National Institute of Standards and Technology, 6 June 2010) <http://www.nist.gov/el/isd/ks/autonomy_levels.cfm>

O’Connell, Mary, ‘Unlawful Killing with Combat Drones: A Case Study of Pakistan, 2004–2009’ (2010) *Notre Dame Law School Legal Studies Research Paper* 2

O’Neil, Cathy, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Penguin Random House, 2016) 24

Oberleitner, Gerd, *Human Rights in Armed Conflict* (Cambridge University Press, 2015) 1

O'Connell, Mary, ‘Banning Autonomous Killing’ in Matthew Evangelista & Henry Shue (eds), *The American Way of Bombing: How Legal and Ethical Norms Change* (Cornell University Press, 2013) 12.

Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts Geneva (1974–1977) (1978) vol 1

Ohlin, Jens David, ‘The Combatant's Stance: Autonomous Weapons on the Battlefield’ (2016) 92 *International Law Studies* 1

Ohlin, Jens, ‘Targeting and the Concept of Intent’ (2013) 35 *Michigan Journal of International Law* 86

Ohlin, Jens, Elies Van Sliedregt and Thomas Weigend, 'Assessing the Control Theory' (2013) 1242 *Cornell Law Faculty Publications Paper* 735

Olasolo, Hector, *Subjective Elements Unlawful Attacks in Combat Situations: From the ICTY's Case Law to the Rome Statute* (Martinus Nijhoff Publishers, 2008) 218

Osinga, Frans, *Science, Strategy and War: The Strategic Theory of John Boyd* (Routledge, 1 edition 2006)

Pagallo, Ugo, 'Robots of Just War: A Legal Perspective' (2011) 24 *Philosophy and Technology* 307, 323.

Parasuraman, Raja, Thomas B Sheridan and Christopher D Wickens, 'A Model for Types and Levels of Human Interaction with Automation' (2000) 30(3) *IEEE Transactions on Systems, Man and Cybernetics* 288

Parks, W Hays, 'Air War and the Law of War' (1990) 32 *Air Force Law Review* 1

Parks, William, 'Conventional Weapons and Weapons Reviews' (2005) 8 *Yearbook of International Humanitarian Law* 55

Parks, William, 'Joint Service Shotgun Program' (1997) *Army Law* 16.

Peruginelli, Gina 'Evaluating Research: the Case of Legal Scholarly Outputs' (2015) 14(2) *Legal Information Management* 50

Petman, Jarna, 'Autonomous Weapons Systems and International Humanitarian Law: Out of the Loop?' (2017) Research Report Ministry for Foreign Affairs of Finland

Pieth, Mark & Radha Ivory, *Corporate Criminal Liability: Emergence, Convergence and Risk* (Springer, 2011) 14

Pilloud, Claud and Jean Pictet, 'Protocol I – Article 49 – Definition of Attacks and Scope of Application' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 601

Pilloud, Claude and Jean Pictet, 'Protocol I – Article 36 – New Weapons' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987)

Pilloud, Claude and Jean Pictet, 'Protocol I – Article 51 – Protection of the Civilian Population' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 613

Pilloud, Claude and Jean Pictet, 'Protocol I – Article 57 – Precautions in Attack' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 677

Piragoff, Donald and Darryl Robinson, 'Article 30, Mental Element' in Otto Triffterer and Kai Ambos (eds), *The Rome Statute of the International Criminal Court A Commentary* (Beck/Hart, 2016) 1122

Pocar, Fausto, 'To What Extent Is Protocol I Customary International Law?' (2002) 78 *International Law Studies* 337

Powles, Steven, 'Joint Criminal Enterprise' (2004) 2 *Journal of International Criminal Justice* 619

Prendergast, David, 'The Constitutionality of Strict Liability in Criminal Law' (2011) 33 *Dublin University Law Journal* 286

Pryer, Douglas A, 'The Rise of the Machines: Why Increasingly "Perfect" Weapons Help to Perpetuate our Wars and Endanger Our Nation' [2013] (March-April) *Military Review* 14

Radin, Sasha and Jason Coats, 'Autonomous Weapon Systems and the Threshold of Non-International Armed Conflict' (2016) 30 *Temple International and Comparative Law Journal* 133

Ratner, Steven et al, *Accountability for Human Rights Atrocities in International Law: Beyond the Nuremburg Legacy* (Oxford University Press, 2009) 355

Rau, Markus, 'State Liability for Violations of International Humanitarian Law — The Distomo Case before the German Federal Constitutional Court' (2006) 7 *German Law Journal* 701

Rauch, Elmar, 'Intervention' (1983) 22 *Military Law and Law of War Review* 291

Reitinger, Nathan, 'Algorithmic Choice and Superior Responsibility: Closing the Gap Between Liability and Lethal Autonomy by Defining the Line Between Actors and Tools' (2015) 51 *Gonzaga Law Review* 118

Richards, Neil M and William D Smart, 'How Should the Law Think about Robots?' in Calo, Ryan, A Michael Froomkin and Ian Kerr (eds), *Robot Law* (Edward Elgar, 2016) 17

Roff, Heather M and Richard Moyes, 'Meaningful Human Control, Artificial Intelligence and Autonomous Weapons' (Briefing paper for delegates at the CCW Meeting of Experts on AWS, Article 36, April 2016)

Roff, Heather, 'Killing in War: Responsibility, Liability and Lethal Autonomous Robots' in Adam Henschke, Nicholas Evans and Fritz Allhoff (eds), *Routledge Handbook of Ethics and War: Just War Theory in the 21st Century* (Routledge Press, 2013) 355

Roff, Heather, 'The Strategic Robot Problem: Lethal Autonomous Weapons in War' (2014) 13(3) *Journal of Military Ethics* 211

Rogers, A P V, 'A Commentary on the Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices' (1987) 26 *Military Law and Law of War Review* 185

Röling, B V A, 'Aspects of the Criminal Responsibility for Violations of the Laws of War' in Antonio Cassese (ed), *The New Humanitarian Law of Armed Conflict* (Napoli: Editoriale Scientifica, 1979) 138

Römer, Jan, *Killing in a Gray Area Between Humanitarian Law and Human Rights: How Can the National Police of Colombia Overcome the Uncertainty of Which Branch of International Law to Apply?* (Springer, 2010) 59

Ronald C, *Governing Lethal Behavior in Autonomous Robots* (Chapman and Hall, 2009)

Ronen, Yael, 'Avoid or Compensate? Liability for Incidental Injury to Civilians Inflicted During Armed Conflict' (2009) 42 *Vanderbilt Journal of Transnational Law* 185

Roorda, Mark, "NATO's Targeting Process: Ensuring Human Control Over and Lawful Use of 'Autonomous' Weapons" (Research Paper No 2015-06, Amsterdam Center for International Law, 2015)

Rousseau, Jean-Jacques, *Of The Social Contract and Other Political Writings* (Penguin, 2012) 51

Rowe, Peter, 'Members of the Armed Forces and Human Rights Law' in Andrew Clapham & Paola Gaeta (eds), *The Oxford Handbook of International Law in Armed Conflict* (Oxford University Press, 2014) 522

Rowley, Jennifer 'Using Case Studies in Research' (2002) 25(1) *Management Research News* 16

Russell, Stuart and Peter Norvig, *Artificial Intelligence A Modern Approach* (Pearson, 2010) 757

Sarkin, Jeremy ‘The Historical Origins, Convergence and Interrelationship of International Human Rights Law, International Humanitarian Law, International Criminal Law and Public International Law and Their Application from at Least the Nineteenth Century’ (2008) *Human Rights and International Legal Discourse, Vol. 1,* [Online] Available: <http://ssrn.com/abstract=1304613> [29 September 2016]

Sassòli, Marco, ‘Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified’ (2014) 90 *International Law Studies* 308

Sassòli, Marco, ‘State Responsibility for Violations of International Humanitarian Law’ (2002) 84 *International Review of the Red Cross* 401

Sassòli, Marco, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare* (Edward Elgar, 2019) 528

Saxon, Dan, ‘A Human Touch: Autonomous Weapons, DoD Directive 3000.09 and the Interpretation of Appropriate Levels of Human Judgment Over the Use of Force’ in Nehal Bhuta, Susanne Beck, Robin Geiβ, Hin Liu, & Claus Kreβ (eds), *Autonomous Weapons Systems: Law, Ethics, Policy* (Cambridge University Press, 2016) 201

Saxon, Dan, ‘A Human Touch: Autonomous Weapons, DOD Directive 3000.09 and the Meaning of Appropriate Levels of Human Judgment over the Use of Force’ (2014) 15(2) *Georgetown Journal of International Affairs* 100.

Saxon, Dan, ‘Closing the Accountability Gap: Individual Criminal Responsibility and Autonomous Weapon Systems’ in Ezio Di Nucci & Flippo Santoni de Sio (eds), *Drones and Responsibility: Legal, Philosophical and Socio-Technical Perspectives on the Use of Remotely Controlled Weapons* (Routledge, 2016) 26

Scharre, Paul, ‘Autonomous Weapons and Operational Risk’ (2016) Ethical Autonomy Project, available online <http://www.cnas.org/sites/default/files/publications-pdf/CNAS_Autonomous-weapons-operational-risk.pdf>

Scharre, Paul, ‘Autonomous Weapons and Operational Risk’ (Center for a New American Security, Ethical Autonomy Project, February 2016)

Schindler, Dietrich & Jiri Toman (eds), *The Laws of Armed Conflicts: A Collection of Conventions, Resolutions, and Other Documents* (Brill – Nijhoff, 4th edition, 2004) 730

Schmitt, Carl, *The Concept of the Political* (University of Chicago Press, 2007) 54

Schmitt, M N, ‘Future War and the Principle of Discrimination’ (1999) 28 *Israel Yearbook on Human Rights* 55

Schmitt, Michael and Widmar, Erik 'On Target': Precision and Balance in the Contemporary Law of Targeting’ (2014) 7 *Journal of National Security and Policy* 379

Schmitt, Michael et al, ‘The Manual on the Law of Non-International Armed Conflict’ (2006) *International Institute of Humanitarian Law*

Schmitt, Michael N (ed), NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013)

Schmitt, Michael N (ed), NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017)

Schmitt, Michael N and Jeffrey S Thurnher, ‘“Out of the Loop”: Autonomous Weapon Systems and the Law of Armed Conflict’ (2013) 4 *Harvard National Security Journal* 231

Schmitt, Michael N, 'Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics' (2013) *Harvard National Security Journal Features* 4

Schmitt, Michael N, 'Fault Lines in the Law of Attack' in Susan C Breau and Agnieszka Jachec-Neale (eds), *Testing the Boundaries of International Humanitarian Law* (British Institute of International and Comparative Law, 2006) 277

Schmitt, Michael N, 'Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance' (2010) 50 *Virginia Journal of International Law* 796

Schmitt, Michael N, 'Precision Attack and International Humanitarian Law' (2005) 87 *International Review of the Red Cross* 445

Schmitt, Michael N, 'The Principle of Discrimination in 21st Century Warfare' (1999) 2 *Yale Human Rights and Development Journal* 143

Schmitt, Michael N, *Essays on Law and War at the Fault Lines* (T M C Asser Press, 2012)

Schmitt, Michael, 'Classification of Cyber Conflict' (2012) 17 *Journal of Conflict and Security Law* 245

Schmitt, Michael, 'Deconstructing Direct Participation in Hostilities: The Constitutive Elements' (2010) 42 *New York University Journal of International Law and Politics* 697

Schmitt, Michael, 'War, Technology, and The Law of Armed Conflict', in Anthony Helm (eds), *The Law of War in the 21st Century: Weaponry and the Use of Force International Law Studies* (Naval War College Press, 2007) 137

Schmitt, Michael, 'Yamasihita, Medina, and Beyond: Command Responsibility in Contemporary Military Operations' (2000) 164 *Military Law Review* 176

Schuller, Alan, ‘At the Crossroads of Control: The Intersection of Artificial Intelligence in Autonomous Weapon Systems with International Humanitarian Law’ (2017) 8 *Harvard National Security Journal* 409

Schulzke, Marcus, ‘Autonomous Weapons and Distributed Responsibility’ (2013) 26 *Philosophy and Technology* 203

Schulzke, Marcus, ‘Robots as Weapons in Just Wars’ (2011) 24 *Philosophy and Technology* 293, 306

Sehrawat, Vivek, ‘Autonomous Weapon System: Law of Armed Conflict (LOAC) and other Legal Challenges’ (2017) 33 *Computer Law & Security Review* 23

Shah, Niaz *Islamic Law and the Law of Armed Conflict: The Conflict in Pakistan* (Routledge, 2011) 35

Shah, Sikander, *International Law and Drone Strikes in Pakistan: The Legal and Socio-Political Aspects* (Routledge, 2014) 183

Sharkey, Noel, ‘Cassandra or False Prophet of Doom: AI Robots and War’ [2008] (July/August) *IEEE Intelligent Systems* 14

Sharkey, Noel, ‘Grounds for Discrimination: Autonomous Robot Weapons’ [2008] (October) *RUSI Defence Systems* 86

Sharkey, Noel, ‘Saying No! to Lethal Autonomous Targeting’ (2010) 9 *Journal of Military Ethics* 369

Sharkey, Noel, ‘The Evitability of Autonomous Robot Warfare’ (2012) 94 *International Review of the Red Cross*

Sharkey, Noel, 'Towards a Principle for the Human Supervisory Control of Robot Weapons' (2014) 2 *Politica & Società* 16

Shelton, Dinah, *Regional Protection of Human Rights* (OUP, 2013) 742

Sheridan, Thomas B and William L Verplank, 'Human and Computer Control of Undersea Teleoperators' (Technical Report, Massachusetts Institute of Technology, 14 July 1978)

Shilo, Liron, 'When Turing Met Grotius AI, Indeterminism, and Responsibility' (9 April 2018). Available at SSRN: <https://ssrn.com/abstract=3280393>

Silberman, Jared 'Non-Lethal Weaponry and Non-Proliferation' (2005) 19 *Notre Dame Journal of Law, Ethics & Public Policy* 352

Simester, AP, 'Can Negligence Be Culpable?' in Jeremy Horder (eds), *Oxford Essays in Jurisprudence* (Oxford University Press, 2000) 85, 106

Simma, Bruno and Andreas Paulus, 'The Responsibility of Individuals for Human Rights Abuses in Internal Conflicts: A Positivist View' (1999) 93 *American Journal of International Law* 302, 316

Simons, Kenneth, 'Dimensions of Negligence in Criminal and Tort Law' (2001) 3 *Theoretical Inquiries in Law* 283, 331

Simons, Kenneth, 'When Is Negligent Advertence Culpable' (2011) 5 *Criminal Law and Philosophy* 97, 112

Simons, Penelope & Audrey Macklin, *The Governance Gap: Extractive Industries, Human Rights, and the Home State Advantage* (Routledge, 2014) 205

Singer, Peter W, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (Penguin Press, 2009)

Singer, Peter, 'In the Loop? Armed Robots and the Future of War' (2009) 1. Available at http://www.brookings.edu/research/articles/2009/01/28-robots-singer.

Singer, Peter, *Corporate Warriors - The Rise of the Privatized Military Industry* (Cornell University Press, 2003) 157

Singer, Peter, *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century* (Penguin, 2009) 229

Singer, Tassilo, 'Update to Revolving Door 2.0: The Extension of the Period for Direct Participation in Hostilities Due to Autonomous Cyber Weapons' (2017) 9th International Conference on Cyber Conflict (CyCon), Tallinn, 1, 13

Sitaropoulos, Nikolaos, 'Weapons and Superfluous Injury or Unnecessary Suffering in International Humanitarian Law: Human Pain in Time of War and the Limits of Law' (2000) *Revue Hellénique de Droit International* 108

Sivakumaran, Sandesh, *The Law of Non-International Armed Conflict* (Oxford University Press, 2012) 263.

Smith, Brian, *The Laws of Manu* (Penguin Classics, 1991) Rule 90-93.

Smith, Keith, *A Modern Treatise on the Law of Criminal Complicity* (Oxford University Press, 1991) 27

Smith, Philip J, C Elaine McCoy and Charles Layton, 'Brittleness in the Design of Cooperative Problem-Solving Systems: The Effects on User Performance' (1997) 27(3) *IEEE Transactions on Systems, Man and Cybernetics* 360

Solis, Gary, *The Law of Armed Conflict: International Humanitarian Law in War* (Cambridge University Press, 2010) 226

Solum, Lawrence B, 'Legal Personhood for Artificial Intelligences' (1992) 70 *North Carolina Law Review* 1231

Sparrow, Robert, 'Can Machines Be People? Reflections on the Turing Triage Test' in Patrick Lin and others (eds), *Robot Ethics: The Ethical and Social Implications of Robotics* (MIT Press, 2012) 301, 305

Sparrow, Robert, 'Killer Robots' (2007) 24 *Journal of Applied Philosophy* 1

Sparrow, Robert, 'Robotic Weapons and the Future of War' in Jessica Wolfendale & Paolo Tripodi (eds), *New Wars and New Soldiers: Military Ethics in the Contemporary World* (Ashgate, 2011) 11

Stark, Findlay, *Culpable Carelessness: Recklessness and Negligence in the Criminal Law* (Cambridge University Press, 2016) 269

Stauffer, Hilary, 'Corporate Liability: An Alternative Path to Accountability?' in Stuart Maslen, Nathalie Weizmann, Maziar Homayounnejad, & Hilary Stauffer (eds), *Drones and Other Unmanned Weapons Systems under International Law* (Brill, 2018) 203

Steinhardt, Ralph, 'Weapons and the Human Rights Responsibilities of Multinational Corporations' in Stuart Casey-Maslen (eds), *Weapons under International Human Rights Law* (Cambridge University Press, 2014) 526

Stephens, Beth, 'Translating Filartiga: A Comparative and International Law Analysis of Domestic Remedies for International Human Rights Violations' (2002) 27 *Yale Journal of International Law* 18

Strachan, Hew and Sibylle Scheipers (eds), *The Changing Character of War* (Oxford University Press, 2011)

Strachan, Hew, 'Surrender in Modern Warfare Since the French Revolution' in Holger Afflerbach & Hew Strachan (eds), *How Fighting Ends: A History of Surrender* (OUP, 2012) 222

Strawser, Bradley, *Killing by Remote Control: The Ethics of an Unmanned Military* (OUP, 2013) 239

Sukman, Daniel, 'Lethal Autonomous Systems and the Future of Warfare' (2015) 16 *Canadian Military Journal* 44

Sullins, John, 'When is a Robot a Moral Agent?' (2006) 6 *International Review of Information Ethics* 23

Swart, Bert, 'Modes of International Criminal Liability' in Antonio Cassese (eds), *The Oxford Companion to International Criminal Justice* (Oxford University Press, 2009) 83, 88

Talmon, Stefan 'The Various Control Tests in the Law of State Responsibility and the Responsibility of Outside Powers for Acts of Secessionist Entities' (2009) 58 *International and Comparative Law Quarterly* [Online] Available: <https://ssrn.com/abstract=1402324> [4 November 2016]

Tarzwell, Amanda, 'In Search of Accountability: Attributing the Conduct of Private Security Contractors to the United States Under the Doctrine of State Responsibility' (2009) 11 *Oregon Review of International Law* 179

Taylor, Greg, 'Concepts of Intention in German Criminal Law' (2014) 24 *Oxford Journal of Legal Studies* 99, 127

Thurnher, Jeffrey S, 'Examining Autonomous Weapon Systems from a Law of Armed Conflict Perspective' in Hitoshi Nasu and Robert McLaughlin (eds), *New Technologies and the Law of Armed Conflict* (Asser Press, 2014) 223

Thurnher, Jeffrey S, 'The Law That Applies to Autonomous Weapon Systems' (2013) 17(4) *ASIL Insights* 1

Thurnher, Jeffrey, 'Feasible Precautions in Attack and Autonomous Weapons' in Wolff Heintschel von Heinegg, Robert Frau, Tassilo Singer (eds), *Dehumanization of Warfare* (Springer, Cham, 2018) 111

Thurnher, Jeffrey, 'Means and Methods of the Future: Autonomous Systems' in Paul Ducheine, Michael Schmitt, Frans Osinga (eds), *Targeting: The Challenges of Modern Warfare* (T.M.C. Asser Press, 2016) 193

Tonkin, Hannah, *State Control over Private Military and Security Companies in Armed Conflict* (*Cambridge University Press*, 2013) 59

Toscano, Christopher, 'Friends of Humans: An Argument for Developing Autonomous Weapons Systems' (2016) 8 *Journal of National Security Law and Policy* 210

Trapp, Kimberley, 'Great Resources Mean Great Responsibility: A Framework of Analysis for Assessing Compliance with API Obligations in the Information Age' in Dan Saxon (eds), *International Humanitarian Law and the Changing Technology of War* (Martinus Nijhoff/Brill, 2013) 156

Trial of the Major War Criminals before the International Military Tribunal, Nuremberg, 14 November 1945 – 1 October 1946 (1947) vol 1

Triffterer, Otto, 'The New International Criminal Law – Its General Principles Establishing International Criminal Responsibility' in Kalliopi Koufa (eds), *The New International Criminal Law* (Sakkoulas Publications, 2003) 706

Truszkowski, Walt et al, 'NASA's Swarm Missions: The Challenge of Building Autonomous Software' (2004) 6(5) *IT Professional Magazine* 47

Tucker, Spencer C, *Instruments of War: Weapons and Technologies That Have Changed History* (ABC-CLIO, 2015)

Uruena, Rene, 'Deciding What is Humane: Towards a Critical Reading of Humanity as a Normative Standard in International Law' in Britta Beers, Luigi Corrias, Wouter Werner (eds), *Humanity Across International Law and Biolaw* (Cambridge University Press, 2014) 183

Van den Boogaard, Jeroen, 'Proportionality and Autonomous Weapons Systems' (2016) 7 *Journal of International Humanitarian Legal Studies* 17

Van Engeland, Anicee, *Civilian or Combatant?: A Challenge for the 21st Century* (Oxford University Press, 2011) 13

van Sliedregt, Elies, *Individual Criminal Responsibility in International Law* (Oxford University Press, 2012)

Verchio, Donna, 'Just Say No! The SIrUS Project: Well-Intentioned, but Unnecessary and Superfluous' (2001) 51 *Air Force Law Review* 183, 213

Vogel, Ryan 'Drone Warfare and the Law of Armed Conflict' (2011) 39(1) *Denver Journal of International Law and Policy* 101

Vyver, Johan, 'The International Criminal Court and the Concept of Mens Rea in International Criminal Law' (2004) 12 *University of Miami International and Comparative Law Review* 57

Wagner, Markus, 'Autonomy in the Battlespace: Independently Operating Weapon Systems and the Law of Armed Conflict' in Saxon, Dan (ed), *International Humanitarian Law and the Changing Technology of War* (Martinus Nijhoff, 2013) 105

Wagner, Markus, 'Taking Humans Out of the Loop: Implications for International Humanitarian Law' (2011) 21(2) *Journal of Law, Information and Science* 155

Wagner, Markus, 'The Dehumanization of International Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapon Systems' (2014) 47 *Vanderbilt Journal of Transnational Law* 1371

Wallach, Wendell and Colin Allen, 'Framing Robot Arms Control' (2013) 15 *Ethics and Information Technology* 125, 133

Wallach, Wendell and Colin Allen, *Moral Machines: Teaching Robots Right from Wrong* (Oxford University Press, 2009)

Wallach, William, Predictability and Lethal Autonomous Weapons Systems (LAWS), IEET (16 April 2016), <https://ieet.org/index.php/IEET2/print/11873>

Wareham, Mary, "Report on Outreach on the UN Report on 'Lethal Autonomous Robotics'" (Report, Campaign to Stop Killer Robots, 31 July 2013) <http://www.stopkillerrobots.org/wpcontent/uploads/2013/03/KRC_ReportHeynsUN_Jul2013.pdf>

Watkin, Kenneth, 'Opportunity Lost: Organized Armed Groups and the ICRC Direct Participation in Hostilities Interpretative Guidance' (2010) 42 *New York University Journal of International Law and Politics* 640

Weigend, Thomas, 'Intent, Mistake of Law, and Co-perpetration in the Lubanga Decision on Confirmation of Charges' (2008) 6 *Journal of International Criminal Justice* 471, 487

Weigend, Thomas, 'Perpetration Through an Organisation: The Unexpected Career of a German Legal Concept' (2011) 9 *Journal of International Criminal Justice* 94, 97

Werle, Gerhard and Florian Jessberger, 'Unless Otherwise Provided: Article 30 of the ICC Statute and the Mental Element of Crimes under International Criminal Law' (2005) 3 *Journal of International Criminal Justice* 35, 53

Werle, Gerhard and Florian Jessberger, *Principles of International Criminal Law* (OUP, 2014) 475

Werle, Gerhard, Boris Burghardt and Claus Roxin, 'Crimes as Part of Organized Power Structures: Introductory Note' (2011) 9 *Journal of International Criminal Justice* 202

Werrell, Kenneth P, *The Evolution of the Cruise Missile* (Air University Press, 1985)

Westen, Peter, 'Individualizing the Reasonable Person in Criminal Law' (2002) 2 *Criminal Law and Philosophy* 137

Weston, Burns H and Jonathan C Carlson, *International Law & World Order: Weston's & Carlson's Basic Documents* (Brill, 2012)

White, Nigel & Sorcha Macleod, 'EU Operations and Private Military Contractors: Issues of Corporate and Institutional Responsibility' (2008) 19 *European Journal of International Law* 966

Whittaker, James A, 'What Is Software Testing? And Why Is It So Hard?' (2000) 17(1) *IEEE Software* 70

Wittes, Benjamin and Gabriella Blum, *The Future of Violence: Robots and Germs, Hackers and Drones* (Basic Books, 2015) 32

Wittes, Benjamin, *Legislating the War on Terror: An Agenda for Reform* (Brookings Institution Press, 2010) 86

Yanev, Lachezar, *Theories of Co-perpetration in International Criminal Law* (Brill-Nijhoff, 2018) 440

Yde, Iben, 'The Push Towards Autonomy: An Insight into the Legal Implications of Self-targeting Weapon Systems' *Royal Danish Defence College* 13.

Zimmermann, Bruno, 'Protocol I – Article 3 – Beginning and End of Application' in Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff, 1987) 65